JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Network Management and Monitoring Guide

Published
2020-09-25

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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 Network Management and Monitoring Guide
Copyright © 2020 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 | lxv

Documentation and Release Notes | **lxv**

Using the Examples in This Manual | **lxv**

- Merging a Full Example | **lxvi**
- Merging a Snippet | **lxvii**

Documentation Conventions | **lxvii**

Documentation Feedback | **lxx**

Requesting Technical Support | **lxx**

- Self-Help Online Tools and Resources | **lxxi**
- Creating a Service Request with JTAC | **lxxi**

1 **Overview**

Network Management Overview | 2

Understanding Device Management Functions in Junos OS | **2**

Understanding Device and Network Management Features | **5**

Understanding Tracing and Logging Operations | **9**

Junos Space Support for Network Management | **11**

- Overview of Junos Space Network Management | **12**
- Preparing the Device for Junos Space Management | **13**

Network Overview | 15

Monitoring Overview | **15**

Diagnostic Tools Overview | **16**

- J-Web Diagnostic Tools | **17**
- CLI Diagnostic Commands | **18**

2

Operation, Administration, and Management Features

Ethernet OAM and Connectivity Fault Management for Routers | 21

Ethernet Operations, Administration, and Maintenance | 21

Introduction to OAM Connectivity Fault Management (CFM) | 22

- Ethernet OAM Connectivity Fault Management | 23
- IEEE 802.1ag OAM Connectivity Fault Management Overview | 24
  - OAM Connectivity Fault Management Overview | 24
  - Connectivity Fault Management Key Elements | 26
  - Best Practices for Configuring 802.1ag Ethernet OAM for VPLS | 28

Configuring Connectivity Fault Management (CFM) | 29

- Creating a Maintenance Domain | 31
- Configuring Maintenance Intermediate Points (MIPs) | 32
- Configuring Maintenance Association Intermediate Points in ACX Series | 33
  - Configuring the Maintenance Domain Bridge Domain | 34
  - Configuring the Maintenance Domain MIP Half Function | 35
  - Configuring the Maintenance Association Intermediate Points with Bridge Domain | 35
  - Configuring the Maintenance Association Intermediate Points with Circuit Cross-Connect | 35
  - Configuring the Maintenance Association Intermediate Points with Bridge Domain when Maintenance Association End Point is Configured | 36
  - Configuring the Maintenance Intermediate Points with Circuit Cross-Connect when Maintenance Association End Point is Configured | 36
- Creating a Maintenance Association | 37
- Continuity Check Protocol Parameters Overview | 38
- Configuring Continuity Check Protocol Parameters for Fault Detection | 39
- Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40
  - Configuring a Maintenance Association End Point (MEP) | 41
  - Configuring a remote Maintenance Association End Point (MEP) | 43
- Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements | 44
- Configuring Service Protection for VPWS over MPLS Using the MEP Interface | 46
- Configuring Linktrace Protocol in CFM | 51

Configuring Rate Limiting of Ethernet OAM Messages | **52**

Configuring Ethernet Local Management Interface | **55**

- Ethernet Local Management Interface Overview | **55**
- Configuring the Ethernet Local Management Interface | **57**
- Example E-LMI Configuration | **59**

Configuring a CFM Action Profile to Specify CFM Actions for CFM Events | **65**

CFM Action Profile to Bring Down a Group of Logical Interfaces Overview | **66**

- Benefits of Creating CFM Action Profile to Bring Down a Group of Logical Interfaces | **67**

Configuring a CFM Action Profile to Bring Down a Group of Logical Interfaces | **67**

Enabling Enhanced Connectivity Fault Management Mode | **71**

Configuring M120 and MX Series Routers for CCC Encapsulated Packets | **73**

- IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview | **73**
- CFM Features Supported on Layer 2 VPN Circuits | **73**
- Configuring CFM for CCC Encapsulated Packets | **74**

Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades | **75**

Configuring Unified ISSU for 802.1ag CFM | **76**

Junos OS Support for Performance Monitoring Compliant with Technical Specification MEF 36 | **79**

Damping CFM performance Monitoring Traps and Notifications to Prevent Congestion of The NMS | **81**

Example: Configuring Ethernet CFM on Physical Interfaces | **81**

Example: Configuring Ethernet CFM on Bridge Connections | **84**

Example: Configuring Ethernet CFM over VPLS | **89**

CFM Monitoring between CE and PE Devices | **100**

Understanding CFM Monitoring between CE and PE Devices | **101**

Single Active Multi-homing Use Case using RDI bit | **102**

Active/Active Multihoming Use case using RDI bit | **102**

Configuring Port Status TLV and Interface Status TLV | **102**

TLVs Overview | **103**

Various TLVs for CFM PDUs | **103**

Support for Additional Optional TLVs | **105**

MAC Status Defects | **112**

Configuring Remote MEP Action Profile Support | **114**

Monitoring a Remote MEP Action Profile | **115**

Configuring Chassis ID TLV | **116**

Configuring MAC Flush Message Processing in CET Mode | **118**

Configuring a Connection Protection TLV Action Profile | **120**

Example: Configuring an Action Profile Based on Connection Protection TLVs | **121**

Configuring Continuity Check Messages | **124**

Configuring Faster Protection Switching for Point-to-Point Network Topologies | **125**

Configuring Faster Convergence for Dual-Homed Multipoint-to-Multipoint Network Topologies | **127**

Configuring a Primary VLAN ID for Increased Flexibility | **128**

Configuring a Remote Maintenance Association to Accept a Different ID | **129**

Link Fault Management for Routers | 131

Introduction to OAM Link Fault Management (LFM) | **131**

IEEE 802.3ah OAM Link-Fault Management Overview | **131**

Understanding Ethernet OAM Link Fault Management for ACX Series Routers | **132**

Configuring Ethernet 802.3ah OAM | **134**

Configuring Link Fault Management | **136**

Configuring Link Discovery | **137**

Configuring the OAM PDU Interval | **138**

Configuring the OAM PDU Threshold | **138**

Configuring Threshold Values for Local Fault Events on an Interface | **138**

Disabling the Sending of Link Event TLVs | **139**

Example: Configuring IEEE 802.3ah OAM Support on an Interface | **139**

Example: Configuring IEEE 802.3ah OAM Support for an Interface on ACX Series | **140**

Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge | **143**

Example: Configuring Ethernet LFM for CCC | **145**

Example: Configuring Ethernet LFM for Aggregated Ethernet | **146**

Configuring an OAM Action Profile | **149**

Specifying the Actions to Be Taken for Link-Fault Management Events | **150**

Monitoring the Loss of Link Adjacency | **151**

Monitoring Protocol Status | **152**

Configuring Threshold Values for Fault Events in an Action Profile | **153**

Applying an Action Profile | **153**

Remote Fault Detection for Link Fault Management | **154**

Detecting Remote Faults | **154**

Enabling Dying Gasp Functionality | **155**

Remote Loopback for Link Fault Management | **156**

Setting a Remote Interface into Loopback Mode | **156**

Enabling Remote Loopback Support on the Local Interface | **157**

Enabling Nonstop Routing for Ethernet Link Fault Management on Backup Routers | **158**

Example: Configuring Ethernet LFM with Loopback Support | **162**

Ethernet Service OAM (ITU-TY.1731) for Routers | 165

ITU-T Y.1731 Ethernet Service OAM Overview | **165**

Ethernet Frame Delay Measurements Overview | **166**

ITU-T Y.1731 Frame Delay Measurement Feature | **166**

One-Way Ethernet Frame Delay Measurement | **168**

Two-Way Ethernet Frame Delay Measurement | **169**

Choosing Between One-Way and Two-Way ETH-DM | **171**

Restrictions for Ethernet Frame Delay Measurement | **171**

Ethernet Frame Loss Measurement Overview | **172**

Service-Level Agreement Measurement | **174**

On-Demand Mode for SLA Measurement | **175**

Proactive Mode for SLA Measurement | **176**

Ethernet Delay Measurements and Loss Measurement by Proactive Mode | **177**

Ethernet Failure Notification Protocol Overview | **177**

Ethernet Synthetic Loss Measurement Overview | **178**

Scenarios for Configuration of ETH-SLM | **179**

Upstream MEP in MPLS Tunnels | **180**

Downstream MEP in Ethernet Networks | **180**

Format of ETH-SLM Messages | **181**

SLM PDU Format | **181**

SLR PDU Format | **181**

Data Iterator TLV Format | **182**

Transmission of ETH-SLM Messages | **182**

Initiation and Transmission of SLM Requests | **183**

Reception of SLMs and Transmission of SLRs | **183**

Reception of SLRs | **184**

Reception of SLRs | **184**

Configuring Ethernet Frame Delay Measurement Sessions | **185**

Guidelines for Configuring Routers to Support an ETH-DM Session | **186**

Configuration Requirements for ETH-DM | **186**

Configuration Options for ETH-DM | **187**

Guidelines for Starting an ETH-DM Session | **187**

ETH-DM Session Prerequisites | **187**

ETH-DM Session Parameters | **188**

Restrictions for an ETH-DM Session | **189**

Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts | **189**

ETH-DM Statistics | **190**

ETH-DM Statistics Retrieval | **192**

ETH-DM Frame Counts | **192**

ETH-DM Frame Count Retrieval | **193**

Configuring Routers to Support an ETH-DM Session | **194**

Configuring MEP Interfaces | **194**

Ensuring That Distributed ppm Is Not Disabled | **195**

Enabling the Hardware-Assisted Timestamping Option | **198**

Configuring the Server-Side Processing Option | 198

Triggering an Ethernet Frame Delay Measurements Session | 199

Starting an ETH-DM Session | 201

Using the monitor ethernet delay-measurement Command | 201

Starting a One-Way ETH-DM Session | 202

Starting a Two-Way ETH-DM Session | 203

Example: Configuring One-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | 204

Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | 210

Managing Continuity Measurement Statistics | 216

Displaying Continuity Measurement Statistics | 216

Clearing Continuity Measurement Statistics | 217

Viewing Ethernet Frame Delay Measurements Statistics | 217

Managing ETH-DM Statistics and ETH-DM Frame Counts | 219

Displaying ETH-DM Statistics Only | 219

Displaying ETH-DM Statistics and Frame Counts | 220

Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity | 220

Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level | 221

Clearing ETH-DM Statistics and Frame Counts | 222

Configuring Ethernet Frame Loss Measurement | 223

Configuring Statistical Frame Loss Measurement for VPLS Connections | 223

Managing ETH-LM Statistics | 224

Displaying ETH-LM Statistics | 225

Clearing ETH-LM Statistics | 226

Example: Measuring Ethernet Frame Loss for Single-Tagged LMM/LMR PDUs | 226

Example: Measuring Ethernet Frame Loss for Dual-Tagged LMM/LMR PDUs | 242

Configuring an Iterator Profile | 257

Configuring an Iterator Profile | 258

Verifying the Configuration of an Iterator Profile | 261

Displaying the Configuration of an Iterator Profile for Two-way Delay Measurement | 261

Displaying the Configuration of an Iterator Profile for Loss Measurement | 262

Displaying the Configuration of a Remote MEP with an Iterator Profile | 263

Disabling an Iterator Profile | 263
Managing Iterator Statistics | 264
Displaying Iterator Statistics | 264
Clearing Iterator Statistics | 270
Configuring a Remote MEP with an Iterator Profile | 270
Configuring Ethernet Synthetic Loss Measurements | 272
Guidelines for Configuring ETH-SLM | 273
Starting a Proactive ETH-SLM Session | 274
Configuring MEP Interfaces | 274
Configuring an Iterator Profile for ETH-SLM | 275
Associating the Iterator Profile with MEPs for ETH-SLM | 277
Starting an On-Demand ETH-SLM Session | 279
Managing ETH-SLM Statistics and ETH-SLM Frame Counts | 280
Displaying ETH-SLM Statistics Only | 280
Displaying ETH-SLM Statistics and Frame Counts | 281
Displaying ETH-SLM Frame Counts for MEPs by Enclosing CFM Entity | 282
Displaying ETH-SLM Frame Counts for MEPs by Interface or Domain Level | 283
Clearing ETH-SLM Statistics and Frame Counts | 284
Clearing Iterator Statistics | 284
Troubleshooting Failures with ETH-SLM | 285
Ethernet Alarm Indication | 286
Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286
Understanding ETH-AIS in a Maintenance Domain | 287
Fault Detection in a Maintenance Domain | 287
Terms Defined | 289
Ethernet Alarm Indication Signal Overview | 291
Configuring ETH-AIS on a CFM MEP | 292
Configuring an Action Profile | 293
Configuring an Action to Be Taken When an AIS Alarm Is Detected | 294
Attaching the Action Profile to a CFM MEP | 295
Configuring Alarm Indication Signal on ACX Series Routers | 297
Inline Transmission Mode | 300
Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling | 301
Enabling Inline Transmission of Link Fault Management Keepalives for Maximum Scaling | 302

Enabling Inline Mode Of Performance Monitoring To Achieve Maximum Scaling | 306

Supported Inline CCM and Inline PM Scaling Values | 309

Enabling the Hardware-Assisted Timestamping Option | 311

Ethernet OAM Connectivity Fault Management for Switches | 312

Understanding Ethernet OAM Connectivity Fault Management for Switches | 312

CFM Limitations on EX4600 Switches | 313

CFM Limitations on QFX5200 Switches and QFX5210 Switches | 314

Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches | 315

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Creating the Maintenance Domain | 321

Configuring the Maintenance Domain MIP Half Function | 322

Creating a Maintenance Association | 322

Configuring the Continuity Check Protocol | 322

Configuring a Maintenance Association End Point | 323

Configuring a Connectivity Fault Management Action Profile | 325

Configuring the Linktrace Protocol | 325

Ethernet OAM Link Fault Management for Switches | 327

OAM Link Fault Management | 327

Understanding Ethernet OAM Link Fault Management | 327

Configuring Ethernet OAM Link Fault Management | 329

Example: Configuring Ethernet OAM Link Fault Management | 331

Ethernet Frame Delay | 336

Understanding Ethernet Frame Delay Measurements on Switches | 336

Ethernet Frame Delay Measurements | 337

Types of Ethernet Frame Delay Measurements | 337

Limitations | 338

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343

Ethernet OAM for Security Devices | 345

Configuring Ethernet OAM Connectivity Fault Management | **345**

Understanding Ethernet OAM Connectivity Fault Management | **345**

Benefits of Ethernet CFM | **347**

CFM over VDSL and PPPoE interfaces for SRX210, SRX220, SRX240, SRX320, SRX340, SRX345, SRX380, SRX550, and SRX550M Devices | **347**

Configuring the Continuity Check Protocol on a Security Device | **348**

Configuring the Link Trace Protocol on a Security Device | **350**

Creating a Maintenance Domain on a Security Device | **350**

Configuring a Maintenance Domain MIP Half Function on a Security Device | **352**

Creating a Maintenance Association on a Security Device | **352**

Configuring a Maintenance Association End Point on a Security Device | **353**

Example: Configuring Ethernet OAM Connectivity Fault Management on a Security Device | **355**

Configuring Ethernet OAM Link Fault Management | **368**

Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways | **368**

Example: Configuring Ethernet OAM Link Fault Management on a Security Device | **370**

Example: Configuring Remote Loopback Mode on VDSL Interfaces on a Security Device | **375**

3 **Uplink Failure Detection**

Uplink Failure Detection Overview | 382

Understanding Uplink Failure Detection | **382**

Uplink Failure Detection Overview | **382**

Failure Detection Pair | **384**

Configuring Uplink Failure Detection | 385

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | **385**

Verifying That Uplink Failure Detection Is Working Correctly | **386**

4 **Network Monitoring Using SNMP**

SNMP Overview | 389

Understanding SNMP Implementation in Junos OS | **389**

SNMP Architecture | **390**

SNMP MIBs | **390**

SNMP Manager and Agent Authentication and Communication | **391**

SNMP Traps and Informs | **391**

SNMP on Junos OS | **392**

Junos OS Support of SNMP Versions | **393**

System Logging Severity Levels for SNMP Traps | **393**

SNMP Communication Flow | **393**

Trap Queuing | **394**

SNMPv3 Overview | **395**

SNMPv3 Overview (QFX in Standalone Mode) | **396**

Loading MIB Files to a Network Management System | **397**

show snmp | **399**

Junos OS SNMP FAQ Overview | **401**

Junos OS SNMP FAQs | **402**

Junos OS SNMP Support FAQs | **403**

Junos OS MIBs FAQs | **404**

Junos OS SNMP Configuration FAQs | **412**

SNMPv3 FAQs | **417**

SNMP Interaction with Juniper Networks Devices FAQs | **419**

SNMP Traps and Informs FAQs | **421**

Junos OS Dual Routing Engine Configuration FAQs | **428**

SNMP Support for Routing Instances FAQs | **429**

SNMP Counters FAQs | **431**

Managing Traps and Informs | **432**

Generating Traps Based on SysLog Events | **432**

Filtering Traps Based on the Trap Category | **433**

Filtering Traps Based on the Object Identifier | **433**

SNMP MIBs and Traps Supported by Junos OS | 436

Enterprise-Specific SNMP MIBs Supported by Junos OS | **436**

Standard SNMP MIBs Supported by Junos OS | **452**

Enterprise-Specific MIBs for Junos OS Evolved on PTX10003 Devices | **479**

Standard MIBs for Junos OS Evolved on PTX10003 Devices | **482**

Standard SNMP Traps Supported by Junos OS | **490**

Standard SNMP Version 1 Traps | **490**

Standard SNMP Version 2 Traps | **494**

Enterprise-Specific SNMP Traps Supported by Junos OS | 500

Juniper Networks Enterprise-Specific SNMP Version 1 Traps | 500

Juniper Networks Enterprise-Specific SNMP Version 2 Traps | 510

Customized SNMP MIBs for Syslog Traps | 521

Overview of Custom SNMP MIBs | 521

Write the MIB File | 522

Convert to a YANG File | 522

CLI Commands to Use for Managing YANG Files | 522

Defining a Custom MIB for a Syslog Trap | 523

Limitations of Using Custom SNMP Traps | 529

Example Custom Syslog Trap | 530

Example Custom Syslog Trap | 537

Configuring Basic SNMP | 544

Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring SNMP | 550

Optimizing the Network Management System Configuration for the Best Results | 555

Changing the Polling Method from Column-by-Column to Row-by-Row | 555

Reducing the Number of Variable Bindings per PDU | 555

Increasing Timeout Values in Polling and Discovery Intervals | 556

Reducing Incoming Packet Rate at the snmpd | 556

Configuring Options on Managed Devices for Better SNMP Response Time | 556

Filtering Out Duplicate SNMP Requests | 557

Excluding Interfaces That Are Slow in Responding to SNMP Queries | 557

Best Practices for Configuring SNMP | 558

Configuring Basic Settings for SNMPv1 and SNMPv2 | 559

Configuring Basic Settings for SNMPv3 | 560

Configuring System Name, Location, Description, and Contact Information | 563

Configuring SNMP on a Device Running Junos OS | 564

Configuring the System Contact on a Device Running Junos OS | 566

Configuring the System Location for a Device Running Junos OS | 567

Configuring the System Description on a Device Running Junos OS | 568

Configuring SNMP Details | 568

Configuring a Different System Name | 571

Configuring the Commit Delay Timer | **571**

Filtering Duplicate SNMP Requests | **572**

Configuring SNMP Communities | **573**

Configuring the SNMP Community String | **577**

Examples: Configuring the SNMP Community String | **578**

Adding a Group of Clients to an SNMP Community | **579**

Configuring a Proxy SNMP Agent | **581**

Configuring SNMP Traps | **583**

Configuring SNMP Trap Options and Groups on a Device Running Junos OS | **585**

Configuring SNMP Trap Options | **586**

- Configuring the Source Address for SNMP Traps | **587**
- Configuring the Agent Address for SNMP Traps | **590**
- Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps | **590**

Configuring SNMP Trap Groups | **591**

SNMP Traps Support | **594**

- SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis | **594**
  - SNMPv1 Traps | **594**
  - SNMPv2 Traps | **600**
- SNMP Traps Supported on QFabric Systems | **605**

Example: Configuring SNMP Trap Groups | **609**

Configuring the Interfaces on Which SNMP Requests Can Be Accepted | **609**

Example: Configuring Secured Access List Checking | **610**

Filtering Interface Information Out of SNMP Get and GetNext Output | **610**

Configuring MIB Views | **612**

Configuring Ping Proxy MIB | **613**

Understanding the Integrated Local Management Interface | **614**

Utility MIB | **615**

SNMP MIBs Support | **616**

- MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis | **616**
- MIBs Supported on QFabric Systems | **626**

MIB Objects for the QFX Series | **633**

- QFX Series Standalone Switches | **633**
- QFabric Systems | **634**
- QFabric System QFX3100 Director Device | **634**

QFabric System QFX3008-I Interconnect Device | 635
QFabric System QFX3600-I Interconnect Device | 636
QFabric System Node Devices | 636
Fabric Chassis MIB | 637
Monitoring RMON MIB Tables | 642
Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 643
Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 646
Example: Configuring SNMP | 648
Configuring RMON Alarms and Events | 652
Configuring SNMP | 653
Configuring an Event | 654
Configuring an Alarm | 654
Configuring SNMPv3 | 656
Minimum SNMPv3 Configuration on a Device Running Junos OS | 657
Example: SNMPv3 Configuration | 658
Creating SNMPv3 Users | 662
Example: Creating SNMPv3 Users | 664
Configuring the SNMPv3 Authentication Type | 665
Configuring MD5 Authentication | 665
Configuring SHA Authentication | 666
Configuring No Authentication | 666
Configuring the SNMPv3 Encryption Type | 667
Configuring the Advanced Encryption Standard Algorithm | 667
Configuring the Data Encryption Algorithm | 668
Configuring Triple DES | 668
Configuring No Encryption | 669
Defining Access Privileges for an SNMP Group | 669
Configuring the Access Privileges Granted to a Group | 671
Configuring the Group | 671
Configuring the Security Model | 671

Configuring the Security Level | 672

Associating MIB Views with an SNMP User Group | 672

Configuring the Notify View | 673

Configuring the Read View | 674

Configuring the Write View | 674

Example: Configuring the Access Privileges Granted to a Group | 674

Assigning Security Model and Security Name to a Group | 676

Configuring the Security Model | 676

Assigning Security Names to Groups | 677

Configuring the Group | 677

Example: Security Group Configuration | 678

Configuring SNMPv3 Traps on a Device Running Junos OS | 678

Configuring the SNMPv3 Trap Notification | 680

Example: Configuring SNMPv3 Trap Notification | 681

Configuring the Trap Notification Filter | 682

Configuring the Trap Target Address | 683

Configuring the Address | 684

Configuring the Address Mask | 684

Configuring the Port | 685

Configuring the Routing Instance | 685

Configuring the Trap Target Address | 685

Applying Target Parameters | 686

Example: Configuring the Tag List | 687

Defining and Configuring the Trap Target Parameters | 688

Applying the Trap Notification Filter | 689

Configuring the Target Parameters | 689

Configuring the Message Processing Model | 690

Configuring the Security Model | 690

Configuring the Security Level | 691

Configuring the Security Name | 691

Configuring SNMP Informs | 692

Configuring the Inform Notification Type and Target Address | 693

Example: Configuring the Inform Notification Type and Target Address | 695

Configuring the Remote Engine and Remote User | 696

Example: Configuring the Remote Engine ID and Remote User | 697

Configuring the Local Engine ID | 701

Configuring the SNMPv3 Community | 703

- Configuring the Community Name | 704
- Configuring the Context | 704
- Configuring the Security Names | 705
- Configuring the Tag | 705

Example: Configuring an SNMPv3 Community | 706

Configuring SNMP for Routing Instances | 710

Understanding SNMP Support for Routing Instances | 710

SNMPv3 Management Routing Instance | 712

- Benefits | 712
- Enabling the Management Routing Instance | 712
- Removing the Management Routing Instance | 712

SNMP MIBs Supported for Routing Instances | 713

Support Classes for MIB Objects | 725

SNMP Traps Supported for Routing Instances | 726

Identifying a Routing Instance | 726

Enabling SNMP Access over Routing Instances | 727

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728

Example: Configuring Interface Settings for a Routing Instance | 729

Configuring Access Lists for SNMP Access over Routing Instances | 731

SNMPv3 Management Routing Instance | 732

- Benefits | 732
- Enabling the Management Routing Instance | 732
- Removing the Management Routing Instance | 733

Configuring SNMP Remote Operations | 734

SNMP Remote Operations Overview | 734

- SNMP Remote Operation Requirements | 735
- Setting SNMP Views | 735
  - Example: Setting SNMP Views | 736

Setting Trap Notification for Remote Operations | 736

Example: Setting Trap Notification for Remote Operations | 737

Using Variable-Length String Indexes | 737

Example: Set Variable-Length String Indexes | 737

Enabling Logging | 737

Using the Ping MIB for Remote Monitoring Devices Running Junos OS | 738

Starting a Ping Test | 739

Before You Begin | 739

Starting a Ping Test | 739

Using Multiple Set PDUs | 740

Using a Single Set PDU | 740

Monitoring a Running Ping Test | 741

pingResultsTable | 741

pingProbeHistoryTable | 743

Generating Traps | 743

Gathering Ping Test Results | 744

Stopping a Ping Test | 746

Interpreting Ping Variables | 746

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747

Starting a Traceroute Test | 747

Using Multiple Set PDUs | 748

Using a Single Set PDU | 748

Monitoring a Running Traceroute Test | 749

traceRouteResultsTable | 749

traceRouteProbeResultsTable | 750

traceRouteHopsTable | 751

Generating Traps | 752

Monitoring Traceroute Test Completion | 753

Gathering Traceroute Test Results | 754

Stopping a Traceroute Test | 756

Interpreting Traceroute Variables | 756

Tracing SNMP Activity | 758

Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | **758**

- Checking for MIB Objects Registered with the snmpd | **758**
- Tracking SNMP Activity | **760**
- Monitoring SNMP Statistics | **762**
- Checking CPU Utilization | **764**
- Checking Kernel and Packet Forwarding Engine Response | **765**

Tracing SNMP Activity on a Device Running Junos OS | **766**

- Configuring the Number and Size of SNMP Log Files | **767**
- Configuring Access to the Log File | **767**
- Configuring a Regular Expression for Lines to Be Logged | **768**
- Configuring the Trace Operations | **768**

Example: Tracing SNMP Activity | **770**

Configure the Certificate Expiration Trap | **770**

Enable Peer Down and IPsec Tunnel Down Traps | **772**

5 **Remote Monitoring (RMON) with SNMP Alarms and Events**

RMON Overview | 774

Understanding RMON | **774**

- RMON Overview | **774**
- Alarm Thresholds and Events | **775**

Understanding RMON Alarms | **777**

- alarmTable | **777**
- jnxRmonAlarmTable | **778**

Understanding RMON Events | **779**

- eventTable | **779**

Understanding RMON Alarms and Events Configuration | **780**

RMON MIB Event, Alarm, Log, and History Control Tables | **781**

Minimum RMON Alarm and Event Entry Configuration | **783**

Configuring an RMON Alarm Entry and Its Attributes | **784**

- Configuring the Alarm Entry | **784**
- Configuring the Description | **785**
- Configuring the Falling Event Index or Rising Event Index | **785**

Configuring the Falling Threshold or Rising Threshold | 786
Configuring the Interval | 786
Configuring the Falling Threshold Interval | 787
Configuring the Request Type | 787
Configuring the Sample Type | 787
Configuring the Startup Alarm | 788
Configuring the System Log Tag | 788
Configuring the Variable | 789
Configuring an RMON Event Entry and Its Attributes | 789
Example: Configuring an RMON Alarm and Event Entry | 790
Configuring RMON History Sampling | 791
Configuring RMON History Sampling Collection | 791
Viewing and Clearing RMON History Statistics | 792
Using alarmTable to Monitor MIB Objects | 793
Creating an Alarm Entry | 794
Configuring the Alarm MIB Objects | 794
alarmInterval | 794
alarmVariable | 795
alarmSampleType | 795
alarmValue | 795
alarmStartupAlarm | 795
alarmRisingThreshold | 795
alarmFallingThreshold | 796
alarmOwner | 796
alarmRisingEventIndex | 796
alarmFallingEventIndex | 796
Activating a New Row in alarmTable | 797
Modifying an Active Row in alarmTable | 797
Deactivating a Row in alarmTable | 797
Using eventTable to Log Alarms | 798
Creating an Event Entry | 798
Configuring the MIB Objects | 798
eventType | 799
eventCommunity | 799

eventOwner | 799

eventDescription | 800

Activating a New Row in eventTable | 800

Deactivating a Row in eventTable | 800

Using RMON to Monitor Network Service Quality | 802

Understanding RMON for Monitoring Service Quality | 802

Setting Thresholds | 803

RMON Command-Line Interface | 804

RMON Event Table | 804

RMON Alarm Table | 805

Troubleshooting RMON | 806

Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806

Measurement Points | 807

Basic Key Performance Indicators | 808

Setting Baselines | 808

Defining and Measuring Network Availability | 809

Defining Network Availability | 809

Monitoring the SLA and the Required Bandwidth | 811

Measuring Availability | 811

Real-Time Performance Monitoring | 812

Measuring Health | 815

Measuring Performance | 822

Measuring Class of Service | 825

Inbound Firewall Filter Counters per Class | 826

Monitoring Output Bytes per Queue | 828

Dropped Traffic | 829

Health Monitoring with SNMP | 831

Understanding Health Monitoring | 831

Configuring Health Monitoring | 832

Configuring Health Monitoring on Devices Running Junos OS | 834

Monitored Objects | 835

Minimum Health Monitoring Configuration | 836

Configuring the Falling Threshold or Rising Threshold | 836

Configuring the Interval | 837

Log Entries and Traps | 837

Example: Configuring Health Monitoring | 837

6

Accounting Options, Source Class Usage, and Destination Class Usage Options

Accounting Options, Source Class Usage and Destination Class Usage Options Overview | 840

Accounting Options Overview | 840

Understanding Source Class Usage and Destination Class Usage Options | 841

Configuring Accounting Options, Source Class Usage and Destination Class Usage Options | 844

Configuration Statements at the [edit accounting-options] Hierarchy Level | 844

Accounting Options Configuration | 846

Accounting Options—Full Configuration | 846

Minimum Accounting Options Configuration | 851

Configuring Accounting-Data Log Files | 856

Configuring How Long Backup Files Are Retained | 857

Configuring the Maximum Size of the File | 858

Configuring Archive Sites for the Files | 858

Configuring Local Backup for Accounting Files | 859

Configuring Files to Be Compressed | 859

Configuring the Maximum Number of Files | 860

Configuring the Storage Location of the File | 860

Configuring Files to Be Saved After a Change in Mastership | 860

Configuring the Start Time for File Transfer | 861

Configuring the Transfer Interval of the File | 861

Managing Accounting Files | 862

Configuring the Interface Profile | 864

Configuring Fields | 865

Configuring the File Information | 865

Configuring Cleared Statistics to be Reported in the Flat File | 865

Configuring the Interval | 866

Example: Configuring the Interface Profile | 866

Configuring the Filter Profile | 868

Configuring the Counters | 868

Configuring the File Information | 869

Configuring the Interval | 869

Example: Configuring a Filter Profile | 870

Example: Configuring Interface-Specific Firewall Counters and Filter Profiles | 871

Configuring SCU or DCU | 873

Creating Prefix Route Filters in a Policy Statement | 874

Applying the Policy to the Forwarding Table | 874

Enabling Accounting on Inbound and Outbound Interfaces | 874

Configuring SCU on a Virtual Loopback Tunnel Interface | 876

Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC | 876

Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface | 877

Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface | 877

Configuring Class Usage Profiles | 878

Configuring a Class Usage Profile | 878

Configuring the File Information | 879

Configuring the Interval | 879

Creating a Class Usage Profile to Collect Source Class Usage Statistics | 880

Creating a Class Usage Profile to Collect Destination Class Usage Statistics | 880

Configuring the MIB Profile | 881

Configuring the File Information | 882

Configuring the Interval | 882

Configuring the MIB Operation | 883

Configuring MIB Object Names | 883

Example: Configuring a MIB Profile | 883

Configuring the Routing Engine Profile | 884

Configuring Fields | 885

Configuring the File Information | 885

Configuring the Interval | 886

Example: Configuring a Routing Engine Profile | 886

7

Monitoring Options

Configuring Interface Alarms | 888

Alarm Overview | **888**

- Alarm Types | **888**
- Alarm Severity | **889**
- Alarm Conditions | **890**
  - Interface Alarm Conditions | **890**
  - System Alarm Conditions | **895**

Example: Configuring Interface Alarms | **896**

Configuring Real-Time Performance Monitoring | 900

RPM Overview | **900**

- RPM Probes | **901**
- RPM Tests | **902**
- Probe and Test Intervals | **902**
- Jitter Measurement with Hardware Timestamping | **902**
- RPM Statistics | **903**
- RPM Thresholds and Traps | **904**
- RPM for BGP Monitoring | **905**

Understanding Real-Time Performance Monitoring on Switches | **906**

- RPM Packet Collection | **906**
- Tests and Probe Types | **907**
- Hardware Timestamps | **907**
- Limitations of RPM on EX Series and QFX Series Switches | **909**

RPM Support for VPN Routing and Forwarding | **910**

RPM Configuration Options | **911**

Two-Way Active Measurement Protocol (TWAMP) Overview | **917**

- Implementation of TWAMP Elements | **918**
- Limitations | **918**

Benefits of TWAMP | 919

Example: Configuring TWAMP Client and Server | 919

Guidelines for Configuring RPM Probes for IPv6 | 926

Configuring the Interface for RPM Timestamping for Client/Server on a Switch (CLI Procedure) | 927

Directing RPM Probes to Select BGP Devices | 930

IPv6 RPM Probes | 930

Configuring IPv6 RPM Probes | 931

Tuning RPM Probes | 932

Monitoring RPM Probes | 933

Example: Configuring Basic RPM Probes | 937

Example: Configuring RPM Using TCP and UDP Probes | 944

Example: Configuring RPM Probes for BGP Monitoring | 948

Configuring IP Monitoring | 952

IP Monitoring Overview | 952

Understanding IP Monitoring Test Parameters | 953

Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups | 954

Example: Configuring IP Monitoring on SRX5000 Series Devices | 955

Example: Configuring IP Monitoring on SRX Series Devices | 962

Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring | 966

Configuring sFlow Monitoring Technology | 970

Overview of sFlow Technology | 970

Overview of sFlow Technology on ACX Series Routers | 973

Understanding How to Use sFlow Technology for Network Monitoring | 975

Benefits of sFlow Technology | 975

Sampling Mechanism and Architecture of sFlow Technology | 975

Adaptive Sampling | 977

How Adaptive Sampling Works | 978

Adaptive Sampling Fallback | 978

Adaptive Sampling Limitations | 979

sFlow Agent Address Assignment | 979

sFlow Limitations on Routers | 980

sFlow Limitations on Switches | 981

Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch | **982**

- Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches | **982**
- Adaptive Sampling | **983**
- sFlow Agent Address Assignment | **984**

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**

Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

Example: Monitoring Network Traffic Using sFlow Technology | **999**

Packet Flow Accelerator Diagnostics Software | 1006

Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities | **1006**

- Understanding External and Internal Ports and Network Interface Card Ports | **1007**
- Understanding Packet Flow Accelerator Diagnostics Software Tests and Scripts | **1008**
- Understanding the ikondiag Command | **1009**
- Understanding Basic Functionality Tests | **1010**
- Understanding and Running Ethernet Tests and Scripts | **1012**
- Understanding and Using Stress Tests | **1018**
- Understanding and Running PTP Tests | **1018**
- Understanding QFX-PFA-4Q Module LED Tests | **1020**
- Understanding Packet Flow Accelerator Diagnostics Utilities | **1021**
- Sample Output for Packet Accelerator Diagnostics Software | **1028**

Installing Ethernet and PTP Scripts | **1036**

- Installing Ethernet and PTP Scripts | **1036**

Installing Packet Flow Accelerator Diagnostics Software | **1038**

- Installing Packet Flow Accelerator Diagnostics Software | **1038**
- Verifying That the QFX-PFA-4Q Expansion Module Is Installed | **1039**
- Downloading the Packet Flow Diagnostics Software | **1040**
- Copying the Packet Flow Diagnostics Software Package to the Switch | **1041**
- Install the Packet Flow Diagnostics Software on the Switch | **1041**
- Configure the Guest VM Options to Launch the Guest VM on the Host | **1043**
- Verifying That the Guest VM is Working | **1046**
- Accessing the Guest VM | **1046**
- Verifying That the FPGA Module Is Working | **1048**
- Validating Connections Between QFX5100-24Q-AA Switch Network Ports and QFX-PFA-4Q Module Ports | **1050**

Uninstalling the Guest VM | **1053**

8

Monitoring Common Security Features

Displaying Real-Time Information from Device to Host | 1057

Displaying Real-Time Monitoring Information | **1057**

Displaying Multicast Path Information | **1060**

Monitoring Security Policies | 1064

Monitoring Security Policy Statistics | **1064**

Monitoring Routing Information | **1065**

- Monitoring Route Information | **1065**
- Monitoring RIP Routing Information | **1068**
- Monitoring OSPF Routing Information | **1069**
- Monitoring BGP Routing Information | **1072**

Monitoring Security Events by Policy | **1074**

Monitoring Security Features | **1077**

- Monitoring Policies | **1077**
- Checking Policies | **1080**
- Monitoring Screen Counters | **1083**
- Monitoring IDP Status | **1086**
- Monitoring Flow Gate Information | **1088**
- Monitoring Firewall Authentication Table | **1089**
- Monitoring Firewall Authentication History | **1091**
- Monitoring 802.1x | **1093**

Monitoring Interfaces and Switching Functions | 1096

Displaying Real-Time Interface Information | **1096**

Monitoring Ethernet Switching | **1099**

Monitoring Interfaces | **1100**

Monitoring PPP | **1102**

Monitoring Events, Services and System | 1103

Monitoring the System | **1103**

- Monitoring System Properties for SRX Series Devices | **1103**
- Monitoring Chassis Information | **1106**

System Health Management for SRX Series Devices | **1107**

Monitoring Unified Threat Management Features | 1110

Monitoring Reports | **1110**

Threats Monitoring Report | **1110**

Traffic Monitoring Report | **1116**

9

Performance Management

Configuring Network Analytics | 1120

Network Analytics Overview | **1120**

Analytics Feature Overview | **1121**

Network Analytics Enhancements Overview | **1122**

Summary of CLI Changes | **1123**

Understanding Enhanced Network Analytics Streaming Data | **1130**

Google Protocol Buffer (GPB) | **1130**

JavaScript Object Notation (JSON) | **1133**

Comma-separated Values (CSV) | **1134**

Tab-separated Values (TSV) | **1134**

Queue Statistics Output for JSON, CSV, and TSV | **1135**

Traffic Statistics Output for JSON, CSV, and TSV | **1135**

Understanding Enhanced Analytics Local File Output | **1137**

Understanding Network Analytics Streaming Data | **1140**

Understanding Network Analytics Configuration and Status | **1143**

Prototype File for the Google Protocol Buffer Stream Format | **1144**

Configuring Queue Monitoring | **1145**

Configuring Traffic Monitoring | **1147**

Configuring a Local File for Network Analytics Data | **1149**

Configuring a Remote Collector for Streaming Analytics Data | **1150**

Example: Configuring Network Analytics | **1152**

Example: Configuring Enhanced Network Analytics Features | **1160**

10

Port Mirroring and Analyzers

Overview of Port Mirroring | 1175

Understanding Port Mirroring and Analyzers | **1175**

- | **1176**
- Port Mirroring Overview | **1176**
- Analyzer Overview | **1177**
- Port-Mirroring Terminology | **1177**
- Port Mirroring Instance Types | **1179**
- Port Mirroring and STP | **1179**
- Port-Mirroring Performance Limitation | **1179**
- Local and Remote Port Mirroring Constraints and Limitations | **1179**
- Remote Port Mirroring Constraints and Limitations | **1181**
- Port Mirroring on OCX Series Switches Constraints and Limitations | **1182**

Understanding Port Mirroring | **1183**

- Port Mirroring Overview | **1183**
- Port-Mirroring Terminology | **1183**

Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches | **1185**

- Port Mirroring Overview | **1185**
- Analyzer Configuration | **1186**
- Port Mirroring and Analyzer Terminologies | **1186**
- Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches | **1188**
- Port-Mirroring Limitation | **1191**

Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches | **1191**

- Port Mirroring Overview | **1192**
- Port Mirroring Terminology | **1193**
- Configuration Guidelines for Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches | **1195**

Understanding Port Mirroring on SRX Devices | **1199**

Understanding Layer 2 Port Mirroring | **1200**

Understanding Layer 2 Port Mirroring Properties | **1201**

- Packet-Selection | **1201**
- Packet Address Family | **1201**

Mirror Destination Properties | **1202**

Mirror-Once Option | **1202**

Application of Layer 2 Port Mirroring Types | **1203**

Restrictions on Layer 2 Port Mirroring | **1205**

Port Mirroring Constraints and Limitations | **1206**

Local and Remote Port Mirroring | **1206**

Remote Port Mirroring Only | **1208**

Port Mirroring on OCX Series Switches | **1209**

Port Mirroring Constraints and Limitations | **1210**

Local and Remote Port Mirroring | **1210**

Remote Port Mirroring Only | **1212**

Port Mirroring on OCX Series Switches | **1213**

Configuring Port Mirroring Analyzers | 1214

Understanding Port Mirroring Analyzers | **1214**

Analyzer Overview | **1215**

Statistical Analyzer Overview | **1216**

Default Analyzer Overview | **1216**

Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers | **1216**

Port Mirroring Analyzer Terminology | **1216**

Configuration Guidelines for Port Mirroring Analyzers | **1218**

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**

Configuring an Analyzer for Local Traffic Analysis | **1222**

Configuring an Analyzer for Remote Traffic Analysis | **1223**

Configuring a Statistical Analyzer for Local Traffic Analysis | **1224**

Configuring a Statistical Analyzer for Remote Traffic Analysis | **1225**

Binding Statistical Analyzers to Ports Grouped at the FPC Level | **1226**

Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups | **1227**

Defining a Next-Hop Group for Layer 2 Mirroring | **1228**

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**

Configuring an Analyzer for Local Traffic Analysis | **1231**

Configuring an Analyzer for Remote Traffic Analysis | **1231**

Configuring Port Mirroring | **1233**

Configuring Port Mirroring to Analyze Traffic (CLI Procedure) | **1234**

- Configuring Port Mirroring for Local Traffic Analysis | **1235**
- Configuring Port Mirroring for Remote Traffic Analysis | **1236**
- Filtering the Traffic Entering an Analyzer | **1237**

Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches | **1238**

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | **1268**

Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches | **1277**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches | **1299**

Configuring Port Mirroring Instances | 1308

Layer 2 Port Mirroring Global Instance | **1308**

Configuring the Global Instance of Layer 2 Port Mirroring | **1309**

Layer 2 Port Mirroring Named Instances | **1312**

- Layer 2 Port Mirroring Named Instances Overview | **1313**
- Mirroring at Ports Grouped at the FPC Level | **1313**
- Mirroring at Ports Grouped at the PIC Level | **1314**
- Mirroring at a Group of Ports Bound to Multiple Named Instances | **1314**

Defining a Named Instance of Layer 2 Port Mirroring | **1315**

Disabling Layer 2 Port Mirroring Instances | **1319**

Configuring Inline Port Mirroring | **1320**

Configuring Port Mirroring for Physical Interfaces | 1322

Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface | **1322**

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level | **1324**

Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level | **1326**

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | **1328**

- Layer 2 Port Mirroring at the FPC Level | **1328**
- Layer 2 Port Mirroring at the PIC Level | **1329**
- Layer 2 Port Mirroring at the FPC and PIC Levels | **1329**

Configuring Layer 2 Port Mirroring Over GRE Interface | **1330**

Example: Configuring Layer 2 Port Mirroring Over a GRE Interface | **1331**

Configuring Port Mirroring for Logical Interfaces | 1339

Layer 2 Port Mirroring Firewall Filters | **1340**

- Layer 2 Port Mirroring Firewall Filters Overview | **1340**
- Mirroring of Packets Received or Sent on a Logical Interface | **1341**
- Mirroring of Packets Forwarded or Flooded to a VLAN | **1341**
- Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance | **1342**

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Defining a Layer 2 Port-Mirroring Firewall Filter | **1346**

Configuring Protocol-Independent Firewall Filter for Port Mirroring | **1349**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1351**

Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces | **1356**

Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces | **1358**

Layer 2 Port Mirroring of PE Router or PE Switch Logical Interfaces | **1359**

Layer 2 Port Mirroring of PE Router or PE Switch Aggregated Ethernet Interfaces | **1361**

Applying Layer 2 Port Mirroring to a Logical Interface | **1363**

Applying Layer 2 Port Mirroring to a Logical Interface | **1367**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | **1370**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1373**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1376**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VLAN | **1379**

Example: Layer 2 Port Mirroring at a Logical Interface | **1382**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1388**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1397**

Configuring Port Mirroring for Multiple Destinations | 1401

Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | **1401**

Defining a Next-Hop Group for Layer 2 Port Mirroring | **1402**

Defining a Next-Hop Group on MX Series Routers for Port Mirroring | **1404**

Example: Configuring Multiple Port Mirroring with Next-Hop Groups on M, MX and T Series Routers | **1407**

Example: Layer 2 Port Mirroring to Multiple Destinations | **1412**

Configuring Port Mirroring for Remote Destinations | 1417

Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN | **1417**

Configuration Layer 2 Port Mirroring to a Remote VLAN | **1418**

- Configuring Port Mirroring to a Remote VLAN | **1418**

Example: Configuring Layer 2 Port Mirroring to Remote VLAN | **1420**

Configuring Port Mirroring Local and Remote Analysis | 1429

Configuring Port Mirroring | **1429**

- Configuring Port Mirroring for Local Analysis | **1430**
- Configuring Port Mirroring for Remote Analysis | **1431**
- Filtering the Traffic Entering an Analyzer | **1432**

Configuring Port Mirroring on SRX Devices | **1433**

Examples: Configuring Port Mirroring for Local Analysis | **1436**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1439**

Example: Configuring Port Mirroring for Local Analysis | **1444**

Example: Configuring Port Mirroring for Remote Analysis | **1450**

Monitoring Port Mirroring | 1457

Displaying Layer 2 Port-Mirroring Instance Settings and Status | **1457**

Displaying Next-Hop Group Settings and Status | **1457**

Troubleshooting Port Mirroring | 1459

Troubleshooting Port Mirroring | **1459**

Port Mirroring Constraints and Limitations | **1459**

Local and Remote Port Mirroring | **1459**

Remote Port Mirroring Only | **1461**

Port Mirroring on OCX Series Switches | **1462**

Egress Port Mirroring with VLAN Translation | **1463**

Egress Port Mirroring with Private VLANs | **1463**

Troubleshooting Port Mirroring Configuration Error Messages | **1464**

An Analyzer Configuration Returns a “Multiple interfaces cannot be configured as a member of Analyzer output VLAN” Error Message | **1464**

11 **System Log Messages**

Overview to System Logging | 1467

Junos OS System Log Overview | **1467**

Overview of Junos OS System Log Messages | **1468**

Junos OS System Log Configuration Hierarchy | **1469**

Junos OS System Logging Facilities and Message Severity Levels | **1470**

Junos OS Default System Log Settings | **1472**

Junos OS Platform-Specific Default System Log Messages | **1473**

Interpreting Messages Generated in Standard Format | **1475**

Managing Host OS System Log and Core Files | **1476**

Viewing Log Files On the Host OS System | **1477**

Copying Log Files From the Host System To the Switch | **1477**

Viewing Core Files On the Host OS System | **1477**

Copying Core Files From the Host System To the Switch | **1478**

Cleaning Up Temporary Files on the Host OS | **1478**

Configuring System Logging for a Single-Chassis System | 1480

Single-Chassis System Logging Configuration Overview | **1480**

Overview of Single-Chassis System Logging Configuration | **1482**

Junos OS System Log Configuration Hierarchy | **1484**

Junos OS System Log Configuration Statements | **1485**

Junos OS Minimum System Logging Configuration | **1486**

Example: Configuring System Log Messages | **1487**

Logging Messages in Structured-Data Format | **1489**

Specifying Log File Size, Number, and Archiving Properties | **1490**

Including Priority Information in System Log Messages | **1492**

System Log Facility Codes and Numerical Codes Reported in Priority Information | **1494**

Including the Year or Millisecond in Timestamps | **1496**

Using Strings and Regular Expressions to Refine the Set of Logged Messages | **1497**

Junos System Log Regular Expression Operators for the match Statement | **1500**

Disabling the System Logging of a Facility | **1501**

Examples: Configuring System Logging | **1502**

Examples: Assigning an Alternative Facility | **1504**

Configuring System Logging for a TX Matrix or TX Matrix Plus Router | 1506

Configuring System Logging for a TX Matrix Router | **1506**

Configuring System Logging for a TX Matrix Plus Router | **1508**

Configuring Message Forwarding to the TX Matrix Router | **1510**

Configuring Message Forwarding to the TX Matrix Plus Router | **1512**

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router | **1513**

Messages Logged When the Local and Forwarded Severity Levels Are the Same | **1513**

Messages Logged When the Local Severity Level Is Lower | **1514**

Messages Logged When the Local Severity Level Is Higher | **1515**

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router | **1516**

Messages Logged When the Local and Forwarded Severity Levels Are the Same | **1516**

Messages Logged When the Local Severity Level Is Lower | **1517**

Messages Logged When the Local Severity Level Is Higher | **1517**

Configuring Optional Features for Forwarded Messages on a TX Matrix Router | **1518**

Including Priority Information in Forwarded Messages | **1519**

Adding a Text String to Forwarded Messages | **1520**

Using Regular Expressions to Refine the Set of Forwarded Messages | **1520**

Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router | **1520**

Including Priority Information in Forwarded Messages | **1521**

Adding a Text String to Forwarded Messages | **1522**

Using Regular Expressions to Refine the Set of Forwarded Messages | **1522**

Configuring System Logging Differently on Each T640 Router in a Routing Matrix | **1522**

Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix | **1524**

Directing System Log Messages to a Remote Destination | 1527

Specifying the Facility and Severity of Messages to Include in the Log | **1527**

Directing System Log Messages to a Log File | **1530**

Directing System Log Messages to a User Terminal | **1531**

Directing System Log Messages to the Console | **1531**

Directing System Log Messages to a Remote Machine or the Other Routing Engine | **1532**

Directing System Log Messages to a Remote Machine | **1533**

Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination | **1534**

Adding a Text String to System Log Messages Directed to a Remote Destination | **1535**

Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination | **1536**

Default Facilities for System Log Messages Directed to a Remote Destination | **1538**

Alternate Facilities for System Log Messages Directed to a Remote Destination | **1538**

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination | **1540**

Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router | **1541**

Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router | **1542**

Displaying System Log Files | 1544

Displaying a Log File from a Single-Chassis System | **1544**

Log File Sample Content | **1545**

Displaying a Log File from a Routing Matrix | **1546**

Displaying and Interpreting System Log Message Descriptions | 1548

Displaying and Interpreting System Log Message Descriptions | **1548**

The message-source Field on a Single-Chassis System | **1550**

The message-source Field on a TX Matrix Platform | **1551**

The message-source Field on a T640 Routing Node in a Routing Matrix | **1553**

Interpreting Messages Generated in Standard Format by a Junos OS Process or Library | **1554**

Interpreting Messages Generated in Standard Format by Services on a PIC | **1555**

Interpreting Messages Generated in Structured-Data Format | **1556**

Examples: Displaying System Log Message Descriptions | **1561**

Configuring System Logging for a Security Device | 1563

Understanding System Logging for Security Devices | **1563**

- Control Plane and Data Plane Logs | **1564**
- Redundant System Log Server | **1564**

Understanding Stream Logging for Security Devices | **1565**

Understanding Binary Format for Security Logs | **1566**

Understanding On-Box Logging and Reporting | **1568**

- Overview | **1568**
- Understanding On-box Logging and Reporting | **1569**
- On-Box Reporting Features | **1571**
- Table Selection | **1572**
- Table Lifetime | **1572**
- Table Dense Mode | **1573**
- Chassis Cluster Scenario | **1573**

Monitoring Reports | **1574**

- Threats Monitoring Report | **1574**
- Traffic Monitoring Report | **1580**

Configuring On-Box Binary Security Log Files | **1582**

Configuring Off-Box Binary Security Log Files | **1584**

Sending System Log Messages to a File | **1586**

Setting the System to Send All Log Messages Through eventd | **1586**

Setting the System to Stream Security Logs | **1587**

Monitoring Log Messages | 1591

Monitoring System Log Messages | **1591**

12 **Network Management and Troubleshooting**

Monitoring and Troubleshooting | 1594

Pinging Hosts | **1594**

Monitoring Traffic Through the Router or Switch | **1595**

- Displaying Real-Time Statistics About All Interfaces on the Router or Switch | **1596**
- Displaying Real-Time Statistics About an Interface on the Router or Switch | **1597**

Dynamic Ternary Content Addressable Memory Overview | **1599**

- Understanding Dynamic Ternary Content Addressable Memory | **1599**
- Applications using Dynamic TCAM Infrastructure | **1599**
- Features Using TCAM Resource | **1600**
- Monitoring TCAM Resource Usage | **1603**
- Example: Monitoring and Troubleshooting the TCAM Resource | **1604**

Service Scaling on ACX5048 and ACX5096 Routers | **1611**

Understanding and Configuring the Unified Forwarding Table | **1611**

- Using the Unified Forwarding Table to Optimize Address Storage | **1612**
- Configuring the Unified Forwarding Table to Optimize Address Storage Using Profiles | **1614**

Troubleshooting and Monitoring TCAM Resource in ACX Series Routers | **1614**

Troubleshooting of System Performance with Resource Monitoring Methodology | 1616

Resource Monitoring Usage Computation Overview | **1616**

- Resource Monitoring and Usage Computation For Trio-Based Line Cards | **1617**
- Resource Monitoring and Usage Computation For I-Chip-Based Line Cards | **1617**

Diagnosing and Debugging System Performance by Configuring Memory Resource Usage Monitoring on MX Series Routers | **1619**

Troubleshooting the Mismatch of jnxNatObjects Values for MS-DPC and MS-MIC | **1622**

Managed Objects for Ukernel Memory for a Packet Forwarding Engine in an FPC Slot | **1624**

Managed Objects for Packet Forwarding Engine Memory Statistics Data | **1624**

Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot | **1625**

jnxPfeMemoryErrorsTable | **1625**

pfeMemoryErrors | **1626**

Configuring Data Path Debugging and Trace Options | 1627

Understanding Data Path Debugging for SRX Series Devices | **1627**

Packet Capture from Operational Mode | **1629**

Understanding Security Debugging Using Trace Options | **1630**

Understanding Flow Debugging Using Trace Options | **1630**

Debugging the Data Path (CLI Procedure) | **1631**

Setting Flow Debugging Trace Options (CLI Procedure) | **1632**

Setting Security Trace Options (CLI Procedure) | **1633**

Displaying Log and Trace Files | **1634**

Displaying Output for Security Trace Options | **1635**

Displaying Multicast Trace Operations | **1636**

J-Web Traceroute Results and Output Summary | **1637**

Displaying a List of Devices | **1638**

Example: Configuring End-to-End Debugging on SRX Series Device | **1640**

Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits | 1646

MPLS Connection Checking Overview | **1646**

Understanding Ping MPLS | **1649**

- MPLS Enabled | **1649**
- Loopback Address | **1649**
- Source Address for Probes | **1649**

Using the ping Command | **1650**

Pinging Layer 2 Circuits | **1653**

Pinging Layer 2 VPNs | **1654**

Pinging Layer 3 VPNs | **1656**

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | **1657**

Using Packet Capture to Analyze Network Traffic | 1659

Packet Capture Overview | **1659**

- Packet Capture on Device Interfaces | **1660**
- Firewall Filters for Packet Capture | **1661**
- Packet Capture Files | **1661**

Analysis of Packet Capture Files | **1662**

Example: Enabling Packet Capture on a Device | **1662**

Example: Configuring Packet Capture on an Interface | **1667**

Example: Configuring a Firewall Filter for Packet Capture | **1670**

Example: Configuring Packet Capture for Datapath Debugging | **1672**

Disabling Packet Capture | **1677**

Deleting Packet Capture Files | **1677**

Changing Encapsulation on Interfaces with Packet Capture Configured | **1679**

Displaying Packet Headers | **1680**

Troubleshooting Security Devices | 1687

Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only) | **1687**

Troubleshooting the Link Services Interface | **1688**

Determine Which CoS Components Are Applied to the Constituent Links | **1688**

Determine What Causes Jitter and Latency on the Multilink Bundle | **1690**

Determine If LFI and Load Balancing Are Working Correctly | **1691**

Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device | **1699**

Troubleshooting Security Policies | **1700**

Synchronizing Policies Between Routing Engine and Packet Forwarding Engine | **1700**

Checking a Security Policy Commit Failure | **1701**

Verifying a Security Policy Commit | **1701**

Debugging Policy Lookup | **1702**

Log Error Messages used for Troubleshooting ISSU-Related Problems | **1702**

Chassisd Process Errors | **1702**

Understanding Common Error Handling for ISSU | **1703**

ISSU Support-Related Errors | **1706**

Initial Validation Checks Failure | **1707**

Installation-Related Errors | **1708**

Redundancy Group Failover Errors | **1709**

Kernel State Synchronization Errors | **1709**

13

Configuration Statements

Configuration Statements: Real-Time Performance Monitoring | 1713

data-fill | **1714**

data-size | **1715**

destination-port | **1717**

dscp-code-point | **1719**

hardware-timestamp | **1721**

history-size | **1722**

moving-average-size | **1723**

one-way-hardware-timestamp | **1724**

port (RPM) | **1725**

probe | **1726**

probe-count | **1729**

probe-interval | **1730**

probe-limit | **1731**

probe-server | **1732**

probe-type | **1733**

routing-instance | **1734**

routing-instance (Syslog) | **1735**

routing-instances | **1736**

rpm (Interfaces) | **1737**

rpm (Services) | **1738**

source-address (Services) | **1742**

tcp | **1743**

test | **1744**

test-interval | **1746**

thresholds (Junos OS) | **1747**

traps | **1749**

udp | **1751**

Configuration Statements: Ethernet OAM Connectivity Fault Management | 1752

802.3ad | **1755**

action-profile (Applying to CFM) | **1756**

action-profile (Defining for CFM) | **1757**

action-profile (MEP) | **1759**

adjacency-loss | **1760**

ais-trigger-condition | **1761**

all-defects | **1762**

auto-discovery | **1763**

avg-fd-twoway-threshold | **1764**

avg-ifdv-twoway-threshold | **1766**

avg-flr-forward-threshold | **1768**

avg-flr-backward-threshold | **1770**

calculation-weight | **1772**

clear-action (CFM) | **1773**

clear oam ethernet connectivity-fault-management event | **1774**

connection-protection-tlv | **1776**

continuity-check | **1777**

convey-loss-threshold | **1778**

cross-connect-ccm | **1779**

cycle-time | **1780**

data-tlv-size | **1781**

default-actions | **1782**

delay | **1783**

delegate-server-processing | **1784**

delay-variation | **1785**

detect-loc | **1786**

direction | **1788**

enhanced-cfm-mode | **1789**

erroneous-ccm | **1790**

evc-protocol cfm | **1791**

event (CFM) | **1793**

flap-trap-monitor | **1794**

hardware-assisted-timestamping | **1796**

hardware-assisted-keepalives | **1797**

hold-interval (OAM) | **1799**

instance | **1800**

interface (IEEE 802.1ag OAM Connectivity-Fault Management) | **1801**

interface (OAM Link-Fault Management) | **1802**

interface-down | **1803**

interface-status-tlv | **1804**

interface-status-send-rdi | **1805**

interval | **1806**

interval (CFM MEP) | **1808**

iteration-count | **1809**

iteration-period | **1810**

level | **1811**

level (CFM MEP) | **1812**

linktrace | **1813**

log-and-generate-ais | **1814**

loss-threshold | **1815**

lowest-priority-defect | **1816**

maintenance-association | **1817**

maintenance-domain | **1819**

measurement-interval | **1821**

measurement-type | **1822**

mep | **1823**

mip-half-function | **1825**

name-format | **1826**

no-aggregate-delegate-processing | **1827**

path-database-size | **1828**

performance-monitoring | **1829**

policer (CFM Global) | **1831**

policer (CFM Session) | **1832**

port-status-tlv | **1833**

priority (Protocols OAM) | **1834**

priority (CFM MEP) | **1835**

priority (OAM Connectivity-Fault Management) | **1836**

protocol (Server MEP) | **1837**

protect-maintenance-association (OAM) | **1838**

rdi | **1839**

receive-ais | **1840**

remote-maintenance-association (OAM) | **1841**

remote-mep | **1842**

sendid-tlv | **1843**

short-name-format | **1844**

sla-iterator-profile | **1845**

sla-iterator-profiles | **1847**

Configuration Statements: Ethernet OAM Link Fault Management | 1849

action (OAM LFM) | **1851**

action (OAM) | **1852**

action-profile (Applying to OAM CFM, for EX Series Switch Only) | **1853**

action-profile | **1855**

age | **1857**

allow-remote-loopback | **1858**

apply-action-profile | **1859**

auto-discovery (EX Series Switch Only) | **1860**

calculation-weight | **1861**

connectivity-fault-management (EX Series Switch Only) | **1862**

continuity-check (EX Series Switch Only) | **1864**

cycle-time | **1865**

delay | **1866**

delay-variation | **1867**

ethernet (Protocols OAM) | **1868**

event (LFM) | **1876**

event-thresholds | **1878**

event-thresholds | **1879**

fast-aps-switch | **1880**

frame-error | **1881**

frame-period | **1882**

frame-period | **1883**

frame-period-summary | **1884**

frame-period-summary | **1885**

hold-interval (OAM CFM, for EX Series Switch Only) | **1886**

hold-interval (OAM) | **1887**

interface (OAM CFM, for EX Series Switch Only) | **1888**

interface (OAM Link-Fault Management) | **1889**

interval (EX Series Switch Only) | **1890**

iteration-period | **1891**

level (EX Series Switch Only) | **1892**

link-adjacency-loss | **1893**

link-discovery | **1894**

link-down | **1895**

link-event-rate | **1896**

link-fault-management | **1897**

negotiation-options | **1899**

no-allow-link-events | **1900**

oam | **1901**

path-database-size (EX Series Switch Only) | **1905**

pdu-interval | **1906**

pdu-threshold | **1907**

performance-monitoring (OAM LFM) | **1908**

protocol-down | **1909**

protocol-down | **1910**

remote-loopback | **1911**

remote-mep (EX Series Switch Only) | **1912**

send-critical-event | **1913**

sla-iterator-profiles (OAM CFM) | **1914**

symbol-period | **1915**

syslog (OAM Action) | **1916**

traceoptions (Individual Interfaces) | **1917**

version-ipfix (Services) | **1926**

Configuration Statements: sFlow Technology | 1928

adaptive-sample-rate | **1929**

agent-id | **1931**

collector | **1932**

disable (sFlow Monitoring Technology) | **1934**

disable-sw-rate-limiter | **1935**

interfaces (sFlow) | **1936**

polling-interval | **1938**

sample-rate | **1940**

sample-rate (QFX Series) | **1942**

sflow | **1943**

source-ip | **1947**

traceoptions (sFlow Technology) | **1948**

udp-port | **1950**

udp-port (QFX Series) | **1951**

Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options | 1952

accounting-options | **1953**

allow-clear (Accounting Options) | **1957**

archive-sites | **1958**

class-usage-profile | **1959**

counters | **1960**

destination-classes | **1961**

fields (for Interface Profiles) | **1962**

fields (for Routing Engine Profiles) | **1964**

file (Associating with a Profile) | **1965**

file (Configuring a Log File) | **1966**

files | **1967**

filter-profile | **1968**

interface-profile | **1969**

interval (Accounting Options) | **1970**

mib-profile | **1971**

mpls (Security Forwarding Options) | **1972**

nonpersistent | **1973**

object-names | **1974**

operation | **1975**

routing-engine-profile | **1976**

size | **1977**

source-classes | **1978**

start-time (Accounting) | **1979**

traceoptions (System Accounting) | **1980**

transfer-interval | **1982**

Configuration Statements: Chassis Cluster | 1983

cluster (Chassis) | **1984**

global-threshold | **1987**

global-weight | **1988**

ip-monitoring | **1989**

ip-monitoring (Services) | **1991**

next-hop | **1993**

Configuration Statements: Datapath Debug | 1994

action-profile | **1995**

capture-file (Security) | **1997**

datapath-debug | **1999**

flow (Security Flow) | **2001**

icmp | **2007**

maximum-capture-size (Datapath Debug) | **2008**

traceoptions (Security Datapath Debug) | **2009**

Configuration Statements: Health Monitoring | 2011

falling-threshold | **2012**

health-monitor | **2013**

health-monitor (KHMS) | **2014**

idp (SNMP) | **2016**

routing-engine (SNMP Resource Level) | **2017**

interval (Health Monitor) | **2019**

rising-threshold | **2020**

Configuration Statements: Remote Monitoring (RMON) | 2021

alarm (SNMP RMON) | **2022**

community | **2023**

description | **2024**

event | 2025

falling-event-index | 2026

falling-threshold | 2027

falling-threshold-interval | 2028

interval | 2029

request-type | 2030

rising-event-index | 2031

rising-threshold | 2032

rmon | 2033

sample-type | 2034

startup-alarm | 2035

syslog-subtag | 2036

type | 2037

variable | 2038

Configuration Statements: Resource Monitoring for Memory Regions | 2039

free-fw-memory-watermark (Resource Monitor) | 2040

free-heap-memory-watermark (Resource Monitor) | 2041

free-nh-memory-watermark (Resource Monitor) | 2042

high-cos-queue-threshold | 2043

high-threshold (Resource Monitor) | 2044

no-load-throttle (Resource Monitor) | 2045

no-logging (Resource Monitor) | 2046

no-throttle (Resource Monitor) | 2047

resource-category jtree (Resource Monitor) | 2048

resource-type (Resource Monitor) | 2050

subscribers-limit (Resource Monitor) | 2052

traceoptions (Resource Monitor) | 2054

Configuration Statements: Security Alarms | 2056

decryption-failures | 2057

idp (Security Alarms) | 2058

Configuration Statements: Network Analytics | 2059

address (Analytics Collector) | **2060**

agent (Analytics) | **2062**

analytics | **2065**

collector (Analytics) | **2072**

depth-threshold | **2074**

export-profiles | **2076**

file (Analytics) | **2079**

inputs (Analytics) | **2081**

interface (Export Profiles) | **2086**

interfaces (Analytics Resource) | **2088**

interfaces (Analytics) | **2090**

latency-threshold | **2092**

local (Analytics Collector) | **2094**

outputs (Analytics) | **2095**

queue-statistics | **2099**

resource (Analytics) | **2101**

resource-profiles (Analytics) | **2103**

service-agents (Analytics) | **2105**

streaming-servers | **2107**

system (Analytics Resource) | **2109**

system (Export Profiles) | **2111**

traceoptions (Analytics) | **2113**

traceoptions (Analytics Agent) | **2114**

traffic-statistics | **2116**

Configuration Statements: SNMP | 2118

access (SNMP) | **2122**

access-list | **2123**

address (SNMP) | **2124**

address-mask | **2125**

agent-address | **2126**

alarm-id | **2127**

alarm (SNMP RMON) | **2128**

alarm-list-name | **2130**

alarm-management | **2131**

alarm-state | **2133**

authentication-md5 | **2135**

authentication-none | **2136**

authentication-password | **2137**

authentication-sha | **2138**

authorization | **2139**

authorization | **2140**

bucket-size | **2141**

categories | **2142**

client-list | **2144**

client-list-name | **2145**

clients | **2146**

commit-delay | **2147**

community (SNMP) | **2148**

community | **2150**

community (RMON) | **2151**

community-name | **2152**

contact (SNMP) | **2153**

customization (SNMP) | **2154**

description | **2155**

description | **2156**

description (RMON) | **2157**

destination-port | **2158**

engine-id | **2159**

enterprise-oid | **2161**

event | **2162**

event | **2163**

falling-event-index | **2164**

falling-event-index (RMON) | **2165**

falling-threshold (Health Monitor) | **2166**

falling-threshold (RMON) | **2167**

falling-threshold | **2168**

falling-threshold-interval | **2169**

falling-threshold-interval | **2170**

filter-duplicates | **2171**

filter-interfaces | **2172**

group (Defining Access Privileges for an SNMPv3 Group) | **2173**

group (Configuring Group Name) | **2174**

health-monitor | **2175**

history | **2176**

interface (SNMP) | **2177**

interface (SNMP RMON History) | **2178**

interval | **2179**

interval (Health Monitor) | **2180**

interval (SNMP RMON) | **2181**

local-engine | **2182**

location (SNMP) | **2183**

logical-system | **2184**

logical-system-trap-filter | **2185**

message-processing-model | **2186**

name | **2187**

nonvolatile | **2188**

notify | **2189**

notify-filter (Applying to the Management Target) | **2190**

notify-filter (Configuring the Profile Name) | **2191**

notify-view | **2192**

oid (SNMPv3) | **2193**

oid | **2194**

owner | **2195**

parameters | **2196**

port | **2197**

privacy-3des | **2198**

privacy-aes128 | **2199**

privacy-des | **2200**

privacy-none | **2201**

privacy-password | **2202**

proxy (snmp) | **2203**

read-view | **2205**

remote-engine | **2206**

request-type | **2208**

request-type | **2209**

retry-count | **2210**

rising-event-index | **2211**

rising-event-index | **2212**

rising-threshold | **2213**

rising-threshold (Health Monitor) | **2214**

rising-threshold (RMON) | **2215**

rmon | **2216**

rmon | **2218**

routing-instance | **2219**

routing-instance-access | **2220**

sample-type | **2221**

sample-type | **2222**

startup-alarm | **2223**

security-level (Defining Access Privileges) | **2224**

security-level (Generating SNMP Notifications) | **2225**

security-model (Access Privileges) | **2226**

security-model (Group) | **2227**

security-model (SNMP Notifications) | **2228**

security-name (Community String) | **2229**

security-name (Security Group) | **2230**

security-name (SNMP Notifications) | **2231**

security-to-group | **2232**

snmp | **2233**

snmp-community | **2240**

snmp-value-match-msmic (Services NAT Options) | **2241**

source-address | **2242**

startup-alarm | **2243**

syslog-subtag | **2244**

syslog-subtag | **2245**

tag (Configuring Notification Targets) | **2246**

tag-list | **2247**

target-address | **2248**

target-parameters | **2250**

targets | **2251**

timeout | **2252**

traceoptions (SNMP) | **2253**

traceoptions (SNMP) | **2256**

trap (Security PKI) | **2258**

trap (Security IKE) | **2260**

trap-group | **2261**

trap-options | **2263**

type (RMON Notification) | **2265**

type | **2266**

type | **2267**

user | **2268**

usm | **2269**

v3 | **2271**

vacm | **2275**

variable | **2276**

variable | **2277**

version (SNMP) | **2278**

view (SNMP Community) | **2279**

view (Configuring a MIB View) | **2280**

write-view | **2281**

Configuration Statements: SNMPv3 | 2282

address | **2284**

address-mask | **2285**

authentication-key | **2286**

authentication-md5 | **2287**

authentication-none | **2288**

authentication-password | **2289**

authentication-sha | **2290**

community-name | **2291**

context (SNMPv3) | **2292**

engine-id | **2293**

group (Configuring Group Name) | **2295**

group (Defining Access Privileges for an SNMPv3 Group) | **2296**

retry-count | **2297**

timeout | **2298**

local-engine | **2299**

message-processing-model | **2300**

notify | **2301**

notify-filter (Applying to the Management Target) | **2302**

notify-filter (Configuring the Profile Name) | **2303**

notify-view | **2304**

oid (SNMPv3) | **2305**

parameters | **2306**

port | **2307**

privacy-3des | **2308**

privacy-aes128 | **2309**

privacy-des | **2310**

privacy-key | **2311**

privacy-none | **2312**

privacy-password | **2313**

read-view | **2314**

remote-engine | **2315**

routing-instance | **2317**

security-level (Defining Access Privileges) | **2318**

security-level (Generating SNMP Notifications) | **2319**

security-model (Access Privileges) | **2320**

security-model (Group) | **2321**

security-model (SNMP Notifications) | **2322**

security-name (Community String) | **2323**

security-name (Security Group) | **2324**

security-name (SNMP Notifications) | **2325**

security-to-group | **2326**

snmp-community | 2327

tag | 2328

tag-list | 2329

target-address | 2330

target-parameters | 2331

type | 2332

user | 2333

usm | 2334

v3 | 2336

vacm | 2340

write-view | 2341

Configuration Statements: Uplink Failure Detection | 2342

action (Uplink Failure Detection) | 2343

group (Uplink Failure Detection) | 2344

link-to-disable | 2345

link-to-monitor | 2346

traceoptions (Uplink Failure Detection) | 2347

uplink-failure-detection | 2349

Cofiguration Statements: Port Mirroring and Analyzers | 2350

analyzer (Port Mirroring) | 2352

analyzer | 2354

bridge-domain (Analyzer) | 2356

disable (Forwarding Options) | 2357

disable-all-instances | 2358

ethernet-switching (Port Mirroring) | 2359

egress | 2360

egress (Analyzer) | 2361

ethernet-switching-options | 2362

family (Port Mirroring) | 2371

family (Port Mirroring) | 2373

forwarding-options | 2375

inet (Port Mirroring) | 2381

ingress (Analyzer) | **2382**

ingress (Port Mirroring) | **2383**

ingress (vlans) | **2384**

input | **2385**

input (Analyzer) | **2387**

input (Port Mirroring) | **2389**

instance | **2390**

instance (Port Mirroring) | **2392**

interface (Analyzer) | **2394**

interface (Next-Hop Group) | **2395**

interface (Port Mirroring) | **2396**

interface (Port Mirroring) | **2397**

ip-address (Port Mirroring) | **2398**

maximum-packet-length | **2399**

mirror-once | **2401**

next-hop-group (Analyzer) | **2402**

next-hop-group (Port Mirroring) | **2403**

no-tag | **2404**

no-tag | **2405**

no-tag | **2406**

no-filter-check | **2407**

no-filter-check | **2408**

output | **2409**

output (Mirroring) | **2410**

output (Port Mirroring) | **2411**

output (Port Mirroring) | **2412**

port-mirroring | **2414**

rate (Forwarding Options) | **2419**

routing-instance | **2421**

routing-instance (Port Mirroring) | **2422**

run-length | **2423**

vlan (Mirroring) | **2424**

vlan (Port Mirroring) | **2425**

vlan (Port Mirroring) | **2426**

Configuration Statements: TWAMP | 2428

twamp-server | **2429**

twamp-client | **2432**

Configuration Statements: Tracing and System Logging | 2435

allow-duplicates | **2437**

archive (All System Log Files) | **2438**

archive (Individual System Log File) | **2440**

cache (Security Log) | **2442**

category (Security Logging) | **2443**

console (System Logging) | **2445**

critical-event (Process) | **2447**

critical-event (System) | **2448**

destination-override | **2449**

event-rate | **2450**

exclude (Security Log) | **2451**

exclude-hostname | **2452**

explicit-priority | **2453**

facility-override (Security) | **2454**

file (Security Log) | **2455**

file (System Logging) | **2457**

files | **2459**

filter (Security) | **2460**

format (Security Log) | **2461**

format (Security Log Stream) | **2462**

host (Security Log) | **2463**

host (System) | **2464**

idle-timeout (System) | **2467**

limit (Security Log) | **2468**

log (Security) | **2469**

log | **2474**

log-prefix (System) | **2476**

log-rotate-frequency | **2477**

major-event (System) | **2478**

major-event (Process) | 2480

match | 2481

match-strings | 2483

memory (System) | 2484

minor-event (Process) | 2486

minor-event (System) | 2487

mode (Security Log) | 2489

no-remote-trace (System) | 2490

pic-services-logging | 2491

port (Syslog) | 2492

process (Memory) | 2493

rate-cap | 2495

rate-limit (Security Log) | 2496

report (Security Log) | 2498

security-log | 2501

security-log-percent-full | 2502

severity (Security Log) | 2503

size (System) | 2504

stream (Security Log) | 2505

structured-data | 2509

syslog (System) | 2510

system (Memory) | 2513

time-format | 2515

trace | 2517

traceoptions (Security Log) | 2519

traceoptions (System) | 2521

tracing | 2523

transport (Security Log) | 2524

ukern-trace | 2525

user (System Logging) | 2526

world-readable | 2527

Configuration Statement: App-Engine | 2528

routing-instance | 2529

14

Operational Commands

Operational Commands: General | 2532

monitor traffic | **2533**

ping | **2549**

request system debug-info | **2557**

show pfe statistics bridge | **2561**

show pfe data | **2567**

show system errors | **2579**

show system errors history | **2583**

traceroute | **2586**

Operational Commands: Realtime Performance Monitoring | 2593

show services rpm active-servers | **2594**

show services rpm history-results | **2596**

show services rpm probe-results | **2601**

Operational Commands: Analyzers and Port Mirroring | 2615

show analyzer | **2616**

Operational Commands: sFlow Monitoring Technology | 2618

clear sflow collectors statistics | **2619**

clear sflow collector statistics (QFX Series) | **2620**

show sflow | **2622**

show sflow collector | **2625**

show sflow interface | **2628**

Operational Commands: Ethernet OAM Connectivity Fault Management | 2632

clear oam ethernet connectivity-fault-management delay-statistics | **2634**

clear oam ethernet connectivity-fault-management sla-iterator-statistics | **2636**

clear oam ethernet connectivity-fault-management statistics | **2638**

clear oam ethernet connectivity-fault-management continuity-measurement | **2640**

clear oam ethernet connectivity-fault-management linktrace path-database | **2642**

clear oam ethernet connectivity-fault-management loss-statistics | **2643**

clear oam ethernet connectivity-fault-management policer | **2645**

clear oam ethernet connectivity-fault-management statistics | 2647

clear oam ethernet connectivity-fault-management synthetic-loss-measurement | 2649

monitor ethernet delay-measurement | 2651

monitor ethernet delay-measurement | 2657

monitor ethernet loss-measurement | 2663

monitor ethernet synthetic-loss-measurement | 2669

monitor ethernet synthetic-loss-measurement | 2674

show oam ethernet connectivity-fault-management delay-statistics | 2679

show oam ethernet connectivity-fault-management forwarding-state | 2684

show oam ethernet connectivity-fault-management forwarding-state | 2689

show oam ethernet connectivity-fault-management interfaces | 2694

show oam ethernet connectivity-fault-management path-database | 2702

show oam ethernet connectivity-fault-management mep-database | 2705

show oam ethernet connectivity-fault-management mip | 2712

show oam ethernet connectivity-fault-management sla-iterator-statistics | 2714

show oam ethernet connectivity-fault-management interfaces | 2727

show oam ethernet connectivity-fault-management linktrace path-database | 2741

show oam ethernet connectivity-fault-management loss-statistics | 2744

show oam ethernet connectivity-fault-management mep-database | 2749

show oam ethernet connectivity-fault-management mep-statistics | 2764

show oam ethernet connectivity-fault-management path-database | 2780

show oam ethernet connectivity-fault-management policer | 2782

show oam ethernet connectivity-fault-management sla-iterator-statistics | 2786

show oam ethernet connectivity-fault-management synthetic-loss-statistics | 2799

show oam ethernet evc | 2802

show oam ethernet fnp interface | 2804

show oam ethernet fnp messages | 2806

show oam ethernet fnp status | 2808

show oam ethernet lmi | 2810

show oam ethernet lmi statistics | 2812

Operational Commands: Ethernet OAM Link Fault Management | 2814

show oam ethernet link-fault-management | 2815

show oam ethernet link-fault-management | 2822

clear oam ethernet link-fault-management state | 2832

clear oam ethernet link-fault-management statistics | 2833

Operational Commands: Uplink Failure Detection | 2834

show uplink-failure-detection | 2835

Operational Commands: RPM | 2837

show services rpm active-servers | 2838

show services rpm history-results | 2840

show services rpm probe-results | 2845

Operational Commands: SNMP | 2859

clear snmp statistics | 2860

request snmp spoof-trap | 2862

show snmp health-monitor | 2870

show snmp inform-statistics | 2879

show snmp mib | 2881

show snmp rmon | 2893

show snmp rmon history | 2899

show snmp statistics | 2904

show snmp v3 | 2912

Operational Commands: Port Mirroring | 2916

show analyzer | 2917

Operational Commands: System Logging | 2919

clear log | 2920

clear security log | 2922

clear security log file | 2924

clear security log stream file | 2925

monitor list | 2927

monitor start | 2929

monitor stop | 2931

request debug information | 2933

show log | 2936

show security log | 2944

show security log file | 2948

show security log severity | 2956

show security log query | 2957

Monitoring Operational Commands | 2960

clear chassis cluster ip-monitoring failure-count | 2962

clear chassis cluster ip-monitoring failure-count ip-address | 2963

clear ilmi statistics | 2965

clear interfaces statistics | 2966

clear services rpm twamp server connection | 2968

clear snmp history | 2969

clear snmp statistics | 2970

request packet-capture start | 2972

request packet-capture stop | 2978

request pppoe connect | 2979

request pppoe disconnect | 2980

request services ip-monitoring preempt-restore policy | 2981

request services rpm twamp start | 2983

request services rpm twamp stop | 2984

request snmp spoof-trap | 2985

request snmp utility-mib set instance | 2993

request snmp utility-mib clear instance | 2994

request support information | 2995

show chassis alarms | 3013

show chassis cluster ip-monitoring status redundancy-group | 3015

show interfaces snmp-index | 3019

show interfaces summary | 3021

show ilmi statistics | 3023

show security alarms | 3028

show security datapath-debug capture | 3034

show security datapath-debug counter | 3036

show security monitoring | 3038

show security monitoring fpc fpc-number | 3041

show security monitoring performance session | 3045

show security monitoring performance spu | 3047

show services ip-monitoring status | 3051

show services rpm twamp client connection | 3056

show services rpm twamp client history-results | 3058

show services rpm twamp client probe-results | 3061

show services rpm twamp client session | 3068

show services rpm twamp server connection | 3070

show services rpm twamp server session | 3072

show snmp health-monitor | 3074

show snmp inform-statistics | 3083

show snmp mib | 3085

show snmp rmon | 3097

show snmp statistics | 3103

show snmp stats-response-statistics | 3111

show snmp v3 | 3114

show system alarms | 3118

show system alarms | 3119

show system khms-stats | 3124

show system monitor memory events | 3131

show system monitor memory status | 3134

show system monitor memory actions | 3137

show system resource-monitor fpc | 3139

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | lxv
- Using the Examples in This Manual | lxv
- Documentation Conventions | lxvii
- Documentation Feedback | lxx
- Requesting Technical Support | lxx

Use this guide for information about the implementation and configuration of various network management technologies that Junos OS supports: Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), Destination Class Usage (DCU) and Source Class Usage (SCU) data, and Accounting Profiles. of alarms, events, and security features are included, as is information on performance management, port mirroring and analyzers, and system logging.

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 lxviii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	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.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

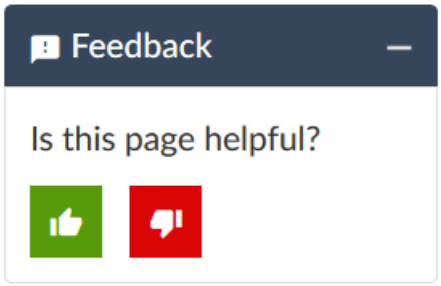
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
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.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- 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/.

1

PART

Overview

Network Management Overview | 2

Network Overview | 15

CHAPTER 1

Network Management Overview

IN THIS CHAPTER

- Understanding Device Management Functions in Junos OS | 2
- Understanding Device and Network Management Features | 5
- Understanding Tracing and Logging Operations | 9
- Junos Space Support for Network Management | 11

Understanding Device Management Functions in Junos OS

After you have installed a device into your network, you need to manage the device within your network. Device management can be divided into five tasks:

- Fault management—Monitor the device; detect and fix faults.
- Configuration management—Configure device attributes.
- Accounting management—Collect statistics for accounting purposes.
- Performance management—Monitor and adjust device performance.
- Security management—Control device access and authenticate users.

The Junos® operating system (Junos OS) network management features work in conjunction with an operations support system (OSS) to manage the devices within the network. Junos OS can assist you in performing these management tasks, as described in Table 3 on page 3.

Table 3: Device Management Features in Junos OS

Task	Junos OS Feature
Fault management	Monitor and see faults using: • Operational mode commands—For more information about operational mode commands, see the CLI Explorer. • SNMP MIBs—For more information about SNMP MIBs supported by Junos OS, see ""Standard SNMP MIBs Supported by Junos OS" on page 452" and ""Enterprise-Specific SNMP MIBs Supported by Junos OS" on page 436. • Standard SNMP traps—For more information about standard SNMP traps, see the "Standard SNMP Traps Supported by Junos OS" on page 490. • Enterprise-specific SNMP traps—For more information about enterprise-specific traps, see ""Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500". • System log messages—For more information about how to configure system log messages, see the *Junos OS Administration Library*. For more information about how to view system log messages, see the System Log Explorer.
Configuration management	• Configure router attributes using the command-line interface (CLI), the Junos XML management protocol, and the NETCONF XML management protocol. For more information about configuring the router using the CLI, see the *Junos OS Administration Library*. For more information about configuring the router using the APIs, see the *Junos XML Management Protocol Guide* and *NETCONF XML Management Protocol Guide*. • Configuration Management MIB—For more information about the Configuration Management MIB, see Configuration Management MIB.

Table 3: Device Management Features in Junos OS *(continued)*

Task	Junos OS Feature
Accounting management	Perform the following accounting-related tasks: • Collect statistics for interfaces, firewall filters, destination classes, source classes, and the Routing Engine. For more information about collecting statistics, see "Accounting Options Configuration" on page 846. • Use interface-specific traffic statistics and other counters, available in the Standard Interfaces MIB, Juniper Networks enterprise-specific extensions to the Interfaces MIB, and media-specific MIBs, such as the enterprise-specific ATM MIB. • Use per-ATM virtual circuit (VC) counters, available in the enterprise-specific ATM MIB. For more information about the ATM MIB, see ATM MIB. • Group source and destination prefixes into source classes and destination classes and count packets for those classes. Collect destination class and source class usage statistics. For more information about classes, see "Destination Class Usage MIB" and "Source Class Usage MIB", "Configuring Class Usage Profiles" on page 878, the *Junos OS Network Interfaces Library for Routing Devices*, and the *Junos OS Routing Protocols Library*. • Count packets as part of a firewall filter. For more information about firewall filter policies, see "Enterprise-Specific SNMP MIBs Supported by Junos OS" on page 436 and the *Junos OS Routing Protocols Library*. • Sample traffic, collect the samples, and send the collection to a host running the CAIDA cflowd utility. For more information about CAIDA and cflowd, see the *Junos OS Routing Protocols Library*.
Performance management	Monitor performance in the following ways: • Use operational mode commands. For more information about monitoring performance using operational mode commands, see the CLI Explorer. • Use firewall filter. For more information about performance monitoring using firewall filters, see the *Junos OS Routing Protocols Library*. • Sample traffic, collect the samples, and send the samples to a host running the CAIDA cflowd utility. For more information about CAIDA and cflowd, see the *Junos OS Routing Protocols Library*. • Use the enterprise-specific Class-of-Service MIB. For more information about this MIB, see Class-of-Service MIB.

Table 3: Device Management Features in Junos OS *(continued)*

Task	Junos OS Feature
Security management	Assure security in your network in the following ways: • Control access to the router and authenticate users. For more information about access control and user authentication, see the *Junos OS Administration Library*. • Control access to the router using SNMPv3 and SNMP over IPv6. For more information, see "Configuring the Local Engine ID" on page 701 and "Tracing SNMP Activity on a Device Running Junos OS" on page 766.

RELATED DOCUMENTATION

Understanding the Integrated Local Management Interface | 614

Understanding SNMP Implementation in Junos OS | 389

Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806

Accounting Options Overview | 840

Understanding Device and Network Management Features

Juniper devices support features that you use to manage the system performance, fault monitoring, and remote access.

Table 4 on page 5 lists the network management features.

Table 4: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 Series

Feature	Typical Uses	Documentation
AI-Scripts and Advanced Insight Manager (AIM)—Automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems, and submit problem reports to Juniper Support Systems.	Fault management	*Advanced Insight Scripts (AI-Scripts) Release Notes*
Alarms and LEDs on the switch—Show status of hardware components and indicate warning or error conditions.	Fault management	*Chassis Alarm Messages on a QFX3500 Device*

Table 4: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 Series *(continued)*

Feature	Typical Uses	Documentation
Firewall filters—Control the packets that are sent to and from the network, balance network traffic, and optimize performance.	Performance management	• *Routing Policies, Firewall Filters, and Traffic Policers User Guide* • *Overview of Firewall Filters (QFX Series)*
In-band management—Enables connection to the switch using the same interfaces through which customer traffic flows. Communication between the switch and a remote console is typically enabled using SSH and Telnet services. SSH provides secure encrypted communications, whereas Telnet provides unencrypted, and therefore less secure, access to the switch.	Remote access management	• *Configuring SSH Service for Remote Access to the Router or Switch* • *Configuring Telnet Service for Remote Access to a Router or Switch*
Juniper Networks Junos OS automation scripts—Configuration and operations automation tools provided by Junos OS. These tools include commit scripts, operation scripts, event scripts, and event policies. Commit scripts enforce custom configuration rules, whereas operation scripts, event policies, and event scripts automate network troubleshooting and management.	• Configuration management • Performance management • Fault management	*Automation Scripting User Guide*
Junos OS command-line interface (CLI)—CLI configuration statements that enable you to configure the switch based on your networking requirements, such as security, service, and performance.	• Configuration management • Performance management • User access management • Remote access management	*Junos OS CLI User Guide*

Table 4: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 Series *(continued)*

Feature	Typical Uses	Documentation
Junos Space software—Multipurpose GUI-based network management system that includes a base platform, the Network Application Platform, and other optional applications such as Ethernet Design, Service Now, Service Insight, and Virtual Control. **NOTE:** Junos Space does not support the OCX Series.	• Configuration management • Performance management • Fault management	• Junos Space Support for Network Management on page 11 • *Junos Space Network Application Platform User Guide*
Junos XML API—XML representation of Junos OS configuration statements and operational mode commands. Junos XML configuration tag elements are the content to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device. The Junos XML API also includes tag elements that are the counterpart to Junos CLI configuration statements.	• Configuration management • Performance management • Fault management	• *Junos XML API Configuration Developer Reference* • *Junos XML API Operational Developer Reference*
NETCONF XML management protocol—XML-based management protocol that client applications use to request and change configuration information on routing, switching, and security platforms running Junos OS. The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as **show**, **set**, and **commit** to perform those operations.	• Configuration management • Performance management • Fault management	*NETCONF XML Management Protocol Developer Guide*

Table 4: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 Series *(continued)*

Feature	Typical Uses	Documentation
Operational mode commands—May be used to do the following: • Monitor switch performance. For example, the **show chassis routing-engine** command shows the CPU utilization of the Routing Engine. High CPU utilization of the Routing Engine can affect performance of the switch. • View current activity and status of the device or network. For example, you can use the **ping** command to monitor and diagnose connectivity problems, and the **traceroute** command to locate points of failure on the network.	• Performance management • Fault management	CLI Explorer
Out-of-band management—Enables connection to the switch through a management interface. Out-of-band management is supported on two dedicated management Ethernet interfaces as well as on the console and auxiliary ports. The management Ethernet interfaces connect directly to the Routing Engine. No transit traffic is allowed through the interfaces, separating customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the switch.	Remote access management	• *Connect a Device to a Network for Out-of-Band Management* • *Connecting a QFX Series Device to a Management Console* • *Configuring Console and Auxiliary Port Properties*

Table 4: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 Series *(continued)*

Feature	Typical Uses	Documentation
SNMP Configuration Management MIB—Provides notification for configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.	Configuration management	SNMP MIB Explorer
SNMP MIBs and traps—Enable the monitoring of network devices from a central location. Use SNMP requests such as **get** and **walk** to monitor and view system activity. The QFX3500 switch supports SNMP Version 1 (v1), v2, and v3, and both standard and Juniper Networks enterprise-specific MIBs and traps.	Fault management	• SNMP MIB Explorer • Understanding SNMP Implementation in Junos OS on page 389
System log messages—Log details of system and user events, including errors. You can specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	• Fault management • User access management	• System Log Explorer • Overview of Junos OS System Log Messages on page 1468 • Overview of Single-Chassis System Logging Configuration on page 1482

Understanding Tracing and Logging Operations

Tracing and logging operations enable you to track events that occur in the switch—both normal operations and error conditions—and to track the packets that are generated by or passed through the switch. The results of tracing and logging operations are placed in files in the **/var/log** directory on the switch.

The Junos OS supports remote tracing for the following processes:

- chassisd—Chassis-control process

- eventd—Event-processing process
- cosd—Class-of-service process

You configure remote tracing by using the **tracing** statement at the **[edit system]** hierarchy level.

> **NOTE:** The **tracing** statement is not supported on the QFX3000 QFabric system.

If you enabled remote tracing but wish to disable it for specific processes on the switch, use the **no-remote-trace** statement at the **[edit *process-name* traceoptions]** hierarchy level. This feature does not alter local tracing functionality in any way, and logging files are stored on the switch.

Logging operations use a system logging mechanism similar to the UNIX syslogd utility to record systemwide, high-level operations, such as interfaces going up or down and users logging in to or out of the switch. You configure these operations by using the **syslog** statement at the **[edit system]** hierarchy level and by using the **options** statement at the **[edit ethernet-switching-options]** hierarchy level.

Tracing operations record more detailed information about the operations of the switch, including packet forwarding and routing information. To configure tracing operations, use the **traceoptions** statement.

> **NOTE:** The **traceoptions** statement is not supported on the QFX3000 QFabric system.

You can define tracing operations in different portions of the switch configuration:

- SNMP agent activity tracing operations—Define tracing of the activities of SNMP agents on the switch. You configure SNMP agent activity tracing operations at the **[edit snmp]** hierarchy level.
- Global switching tracing operations—Define tracing for all switching operations. You configure global switching tracing operations at the **[edit ethernet-switching-options]** hierarchy level of the configuration.
- Protocol-specific tracing operations—Define tracing for a specific routing protocol. You configure protocol-specific tracing operations in the **[edit protocols]** hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global **traceoptions** statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.
- Tracing operations within individual routing protocol entities—Some protocols allow you to define more granular tracing operations. For example, in Border Gateway Protocol (BGP), you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.

- Interface tracing operations—Define tracing for individual interfaces and for the interface process itself. You define interface tracing operations at the **[edit interfaces]** hierarchy level of the configuration.
- Remote tracing—To enable system-wide remote tracing, configure the **destination-override syslog host** statement at the **[edit system tracing]** hierarchy level. This specifies the remote host running the system log process (syslogd), which collects the traces. Traces are written to files on the remote host in accordance with the syslogd configuration in **/etc/syslog.conf**. By default, remote tracing is not configured.

  To override the system-wide remote tracing configuration for a particular process, include the **no-remote-trace** statement at the **[edit *process-name* traceoptions]** hierarchy. When **no-remote-trace** is enabled, the process does local tracing.

  To collect traces, use the local0 facility as the selector in the **/etc/syslog.conf** file on the remote host. To separate traces from various processes into different files, include the process name or trace-file name (if it is specified at the [edit ***process-name* traceoptions file**] hierarchy level) in the Program field in the **/etc/syslog.conf** file. If your system log server supports parsing hostname and program name, then you can separate traces from the various processes.

  NOTE: During a commit check, warnings about the **traceoptions** configuration (for example, mismatch in trace file sizes or number of trace files) are not displayed on the console. However, these warnings are logged in the system log messages when the new configuration is committed.

RELATED DOCUMENTATION

Overview of Junos OS System Log Messages | **1468**

Junos Space Support for Network Management

IN THIS SECTION

- Overview of Junos Space Network Management | **12**
- Preparing the Device for Junos Space Management | **13**

The Juniper Networks Junos Space application, running on a JA1500 appliance or a Junos Space Virtual Appliance, is a comprehensive platform for building and deploying applications for collaboration, productivity,

and network infrastructure and operations management. Junos Space provides a runtime environment implemented as a fabric of virtual and physical appliances.

The following subsections describe Junos Space support for network management”

Overview of Junos Space Network Management

The Junos Space Network Management Platform software comprises various applications for network management and configuration, including:

- Junos Space Administration—Provides management of Junos Space fabric, databases, licenses, applications, authentication servers, tags, permission labels, DMI schemas, and troubleshooting.
- Network Director—Provides unified management of supported Juniper Networks devices in your network. By providing full network life cycle management, Network Director simplifies the discovery, configuration, visualization, monitoring, and administration of large networks.
- Service Automation—Provides an end-to-end solution designed to streamline operations and enable proactive network management for Junos OS devices. The solution consists of Advanced Insight Scripts (AI-Scripts), Junos Space Service Now and Service Insight applications, and Juniper Support Systems (JSS).

> **NOTE:** Do not install Junos Space and AI-Scripts on the control plane network EX4200 switches or EX4200 Virtual Chassis in a QFX3000 QFabric system

Before you can use Junos Space Network Director to manage the QFX Series device, you must ensure that the configuration on the device meets the requirements for all managed devices. For example:

- The device configuration has a static management IP address that is reachable from the Junos Space server.
- There is a user with full administrative privileges for Junos Space administration.
- SNMP is enabled (only if you plan on using SNMP as part of the device discovery).
- In Junos Space, set up a default device management interface (DMI) schema for the QFX Series device.

For more information about Network Director requirements, see the *Network Director Quick Start Guide* at:

https://www.juniper.net/documentation/en_US/network-director1.5/information-products/pathway-pages/index.html

For more information about Junos Space, go to:

https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html

Preparing the Device for Junos Space Management

Before you can use the Juniper Networks Junos Space application to manage the QFX Series device, you must ensure that the configuration on the device meets the following requirements for device discovery in Junos Space:

- The device configuration has a static management IP address that is reachable from the Junos Space server.
- There is a user with full administrative privileges for Junos Space administration.
- SNMP is enabled (only if you plan on using SNMP as part of the device discovery).
- In Junos Space, set up a default device management interface (DMI) schema for the QFX Series device.

> **NOTE:** Do not install Junos Space and AI-Scripts (AIS) on the control plane network EX4200 switches or EX4200 Virtual Chassis in a QFX3000 QFabric system

To prepare the device before using Junos Space:

1. Perform the initial configuration of the device through the console port using the Junos OS CLI. This task includes the configuration of a static management IP address and a user with root administrative privileges.

   For the QFX3500 switch, see *Configuring a QFX3500 Device as a Standalone Switch*.

   For the QFabric system, see *QFabric System Initial and Default Configuration Information* and *Performing the QFabric System Initial Setup on a QFX3100 Director Group*.

2. (Optional) Configure SNMP if you plan on using SNMP to probe devices during device discovery.

   See "Configuring SNMP" on page 550.

3. (Optional) Enable SSH if you wish to use the Secure Console feature in Junos Space.

   See *Configuring SSH Service for Remote Access to the Router or Switch*.

4. In Junos Space, set up a default DMI schema. For more information about managing DMI schemas, see:

   https://www.juniper.net/documentation/en_US/junos-space13.1/platform/information-products/pathway-pages/junos-space-administration-pw.html
   .

RELATED DOCUMENTATION

Configuring a QFX3500 Device as a Standalone Switch

QFabric System Initial and Default Configuration Information

Performing the QFabric System Initial Setup on a QFX3100 Director Group

RELATED DOCUMENTATION

Configuring SNMP | **550**

Configuring SSH Service for Remote Access to the Router or Switch

CHAPTER 2

Network Overview

IN THIS CHAPTER

- Monitoring Overview | 15
- Diagnostic Tools Overview | 16

Monitoring Overview

Junos OS supports a suite of J-Web tools and CLI operational mode commands for monitoring the system health and performance of your device. Monitoring tools and commands display the current state of the device. To use the J-Web user interface and CLI operational tools, you must have the appropriate access privileges.

You can use the J-Web Monitor option to monitor a device. J-Web results appear in the browser.

You can also monitor the device with CLI operational mode commands. CLI command output appears on the screen of your console or management device, or you can filter the output to a file. For operational commands that display output, such as the **show** commands, you can redirect the output into a filter or a file. When you display help about these commands, one of the options listed is **|**, called a *pipe*, which allows you to filter the command output.

For example, if you enter the **show configuration** command, the complete device configuration appears on the screen. To limit the display to only those lines of the configuration that contain **address**, enter the **show configuration** command using a pipe into the **match** filter:

```
user@host> show configuration | match address
```

```
address-range low 192.168.3.2 high 192.168.3.254;
address-range low 192.168.71.71 high 192.168.71.254;
address 192.168.71.70/21;
address 192.168.2.1/24;
address 127.0.0.1/32;
```

For a complete list of the filters, type a command, followed by the pipe, followed by a question mark (?):

```
user@host> show configuration | ?
```

```
Possible completions:
compare             Compare configuration changes with prior version
count               Count occurrences
display             Show additional kinds of information
except              Show only text that does not match a pattern
find                Search for first occurrence of pattern
hold                Hold text without exiting the prompt
last                Display end of output only
match               Show only text that matches a pattern
no-more             Don't paginate output
request             Make system-level requests
resolve             Resolve IP addresses
save                Save output text to file
trim                Trim specified number of columns from start of line
```

You can specify complex expressions as an option for the **match** and **except** filters.

NOTE: To filter the output of configuration mode commands, use the filter commands provided for the operational mode commands. In configuration mode, an additional filter is supported.

RELATED DOCUMENTATION

Monitoring Interfaces | 1100

Diagnostic Tools Overview | 16

Diagnostic Tools Overview

IN THIS SECTION

J-Web Diagnostic Tools | 17

CLI Diagnostic Commands | 18

Juniper Networks devices support a suite of J-Web tools and CLI operational mode commands for evaluating system health and performance. Diagnostic tools and commands test the connectivity and reachability of hosts in the network.

- Use the J-Web Diagnose options to diagnose a device. J-Web results appear in the browser.
- Use CLI operational mode commands to diagnose a device. CLI command output appears on the screen of your console or management device, or you can filter the output to a file.

To use the J-Web user interface and CLI operational tools, you must have the appropriate access privileges.

This section contains the following topics:

J-Web Diagnostic Tools

The J-Web diagnostic tools consist of the options that appear when you select **Troubleshoot** and **Maintain** in the task bar. Table 5 on page 17 describes the functions of the Troubleshoot options.

Table 5: J-Web Interface Troubleshoot Options

Option	Function
Troubleshoot Options	
Ping Host	Allows you to ping a remote host. You can configure advanced options for the ping operation.
Ping MPLS	Allows you to ping an MPLS endpoint using various options.
Traceroute	Allows you to trace a route between the device and a remote host. You can configure advanced options for the traceroute operation.
Packet Capture	Allows you to capture and analyze router control traffic.
Maintain Options	
Files	Allows you to manage log, temporary, and core files on the device.
Upgrade	Allows you to upgrade and manage Junos OS packages.
Licenses	Displays a summary of the licenses needed and used for each feature that requires a license. Allows you to add licenses.
Reboot	Allows you to reboot the device at a specified time.

CLI Diagnostic Commands

The CLI commands available in operational mode allow you to perform the same monitoring, troubleshooting, and management tasks you can perform with the J-Web user interface. Instead of invoking the tools through a graphical interface, you use operational mode commands to perform the tasks.

You can perform certain tasks only through the CLI. For example, you can use the **mtrace** command to display trace information about a multicast path from a source to a receiver, which is a feature available only through the CLI.

To view a list of top-level operational mode commands, type a question mark (?) at the command-line prompt.

At the top level of operational mode are the broad groups of CLI diagnostic commands listed in Table 6 on page 18.

Table 6: CLI Diagnostic Command Summary

Command	Function
Controlling the CLI Environment	
set *option*	Configures the CLI display.
Diagnosis and Troubleshooting	
clear	Clears statistics and protocol database information.
mtrace	Traces information about multicast paths from source to receiver.
monitor	Performs real-time debugging of various Junos OS components, including the routing protocols and interfaces.
ping	Determines the reachability of a remote network host.
ping mpls	Determines the reachability of an MPLS endpoint using various options.
test	Tests the configuration and application of policy filters and AS path regular expressions.
traceroute	Traces the route to a remote network host.
Connecting to Other Network Systems	
ssh	Opens secure shell connections.
telnet	Opens Telnet sessions to other hosts on the network.

Table 6: CLI Diagnostic Command Summary *(continued)*

Command	Function
Management	
copy	Copies files from one location on the device to another, from the device to a remote system, or from a remote system to the device.
restart ***option***	Restarts the various system processes, including the routing protocol, interface, and SNMP processes.
request	Performs system-level operations, including stopping and rebooting the device and loading Junos OS images.
start	Exits the CLI and starts a UNIX shell.
configuration	Enters configuration mode.
quit	Exits the CLI and returns to the UNIX shell.

RELATED DOCUMENTATION

MPLS Connection Checking Overview | **1646**

Understanding Ping MPLS | **1649**

Using the J-Web Ping Host Tool

Using the ping Command | **1650**

PART 2

Operation, Administration, and Management Features

Ethernet OAM and Connectivity Fault Management for Routers | **21**

Link Fault Management for Routers | **131**

Ethernet Service OAM (ITU-TY.1731) for Routers | **165**

Ethernet OAM Connectivity Fault Management for Switches | **312**

Ethernet OAM Link Fault Management for Switches | **327**

Ethernet Frame Delay | **336**

Ethernet OAM for Security Devices | **345**

CHAPTER 3

Ethernet OAM and Connectivity Fault Management for Routers

IN THIS CHAPTER

- Ethernet Operations, Administration, and Maintenance | 21
- Introduction to OAM Connectivity Fault Management (CFM) | 22
- Configuring Connectivity Fault Management (CFM) | 29
- CFM Monitoring between CE and PE Devices | 100
- Configuring Continuity Check Messages | 124

Ethernet Operations, Administration, and Maintenance

This topic provides an overview to help you effectively configure Ethernet Operations, Administration, and Maintenance (OAM) on a network of Juniper Networks® MX Series 5G Universal Routing Platforms.

Ethernet OAM provides the tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual local area network (VLAN) identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports, or a virtual service such as pseudowire, and so on.
- Isolate faults over a flat (or single operator) network architecture or a nested or hierarchical (or multi-provider) network.

OAM can provide simple link-level information, provide performance statistics, or track end-to-end connectivity across the network. Simple link fault management (LFM) for Ethernet links is defined in IEEE 802.3ah.

IEEE 802.1ag OAM is supported on untagged, single tagged, and stacked VLAN interfaces.

Ethernet OAM functions are implemented as:

- Fault detection and notification (provided by continuity check messages)

- Path discovery (provided by the linktrace protocol)
- Fault isolation, verification, and recovery (isolation and verification are provided by a combination of protocols, while recovery is the function of protocols such as spanning tree)

The loopback protocol used in Ethernet OAM is modeled on the standard IP ping. After a fault is detected, the loopback protocol performs fault verification and isolation under the direction of a network operator.

The loopback is performed using request and response message pairs. A unicast loopback message is generated by a maintenance endpoint (MEP), and a loopback reply is generated by the destination maintenance intermediate point (MIP) or MEP.

The target MAC address is learned by the continuity check protocol or linktrace protocol. The loopback message's packet is always forwarded to a unique port by the originating MEP, as determined by a MAC table lookup or the MEP interface MAC address.

The target MIP or MEP generates a unicast loopback reply in response to the received loopback message. The loopback message follows the same path as a data packet, and intermediate bridges simply forward the packet to the destination MIP or MEP.

RELATED DOCUMENTATION

Ethernet OAM Connectivity Fault Management | 23

Example: Configuring Ethernet CFM on Bridge Connections | 84

Example: Configuring Ethernet CFM on Physical Interfaces | 81

Introduction to OAM Connectivity Fault Management (CFM)

IN THIS SECTION

Ethernet OAM Connectivity Fault Management | 23

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

Use this topic to understand more about the connectivity fault management (CFM).

Ethernet OAM Connectivity Fault Management

The most complete connectivity fault management (CFM) is defined in IEEE 802.1ag. This topic emphasizes the use of CFM in a Metro Ethernet environment.

The major features of CFM are:

- Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
- Path discovery and fault verification using the linktrace protocol. Similar to IP traceroute, this protocol maps the path taken to a destination MAC address through one or more bridged networks between the source and destination.
- Fault isolation using the loopback protocol. Similar to IP ping, this protocol works with the continuity check protocol during troubleshooting.

CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains.

Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible. Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outermost domains are assigned a higher level than the innermost domains.

Customer end points have the highest maintenance domain level. In a CFM maintenance domain, each service instance is called a maintenance association. A *maintenance association* can be thought as a full mesh of maintenance endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages.

There is also a maintenance intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

MEPs can be *up MEPs* or *down MEPs*. A link can connect a MEP at level 5 to a MEP at level 7. The interface at level 5 is an up MEP (because the other end of the link is at MEP level 7), and the interface at level 7 is a down MEP (because the other end of the link is at MEP level 5).

In a Metro Ethernet network, CFM is commonly used at two levels:

- By the service provider to check the connectivity among its provider edge (PE) routers
- By the customer to check the connectivity among its customer edge (CE) routers

> **NOTE:** The configured customer CFM level must be greater than service provider CFM level.

In many Metro Ethernet networks, CFM is used to monitor connectivity over a VPLS and bridge network.

> **NOTE:** In ACX Series routers, OAM for VPLS is supported only on ACX5048, ACX5096, and ACX5448 routers.

SEE ALSO

CFM Monitoring between CE and PE Devices | **100**

Configuring Continuity Check Messages | **124**

IEEE 802.1ag OAM Connectivity Fault Management Overview

IN THIS SECTION

- OAM Connectivity Fault Management Overview | **24**
- Connectivity Fault Management Key Elements | **26**
- Best Practices for Configuring 802.1ag Ethernet OAM for VPLS | **28**

Ethernet interfaces on M7i and M10i routers with the Enhanced CFEB (CFEB-E) and on M120, M320, MX Series, T Series, and PTX Series routers support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM). The goal of CFM is to monitor an Ethernet network that may comprise one or more service instances. Junos OS supports IEEE 802.1ag connectivity fault management.

> **NOTE:** MX Series Virtual Chassis does not support distributed inline connectivity fault management.
>
> ACX Series routers support CFM on aggregated Ethernet interfaces with continuity check interval of 100 milliseconds or higher.

OAM Connectivity Fault Management Overview

In Junos OS Release 9.3 and later, CFM also supports aggregated Ethernet interfaces. Connectivity fault management (CFM) sessions operate in distributed mode and are processed on the Flexible PIC Concentrator

(FPC) on aggregated Ethernet interfaces. As a result, graceful Routing Engine switchover (GRES) is supported on aggregated Ethernet interfaces. In releases before Junos OS Release 13.3, CFM sessions operate in centralized mode and are processed on the Routing Engine. However, CFM sessions are not supported on aggregated Ethernet interfaces if the interfaces that form the aggregated Ethernet bundle are in mixed mode. CFM sessions with a continuity check message (CCM) interval of 10 milliseconds are not supported over aggregated Ethernet interfaces.

CFM sessions are distributed by default. All CFM sessions must operate in either only distributed or only centralized mode. A mixed operation of distributed and centralized modes for CFM sessions is not supported. To disable the distribution of CFM sessions on aggregated Ethernet interfaces and make the sessions operate in centralized mode, include the **no-aggregate-delegate-processing** statement at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

NOTE: As a requirement for Ethernet OAM 802.1ag to work, distributed periodic packet management (PPM) runs on the Routing Engine and Packet Forwarding Engine. You can only disable PPM on the Packet Forwarding Engine. To disable PPM on the PFE, include the **ppm no-delegate-processing** statement at the **[edit routing-options ppm]** hierarchy level.

NOTE:

- CFM sessions are supported on aggregated Ethernet interfaces if the interfaces that form the aggregated Ethernet bundle are in mixed mode when the **no-aggregate-delegate-processing** command is enabled.
- Starting in Junos OS Release 14.2, for CFM sessions in centralized mode, we recommend that you configure a maximum of 40 CFM sessions with continuity check message (CCM) interval of 100 milliseconds (100 ms) or a maximum of 400 CFM sessions with CCM interval of 1 second (1 s). If CFM sessions are configured beyond this limit, CFM might not work as expected. You might observe issues when the state of multiple links change or when the line cards are restarted.

  Note that these limits have been derived by considering a protocol data unit (PDU) load of 400 packets per second (pps) on the Routing Engine. This limit varies depending on the Routing Engine load. If the Routing Engine experiences heavy load, expect some variations to this limit.

Starting in Junos OS Release 10.3, on interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers, CFM is not supported on untagged aggregated Ethernet member links. MPCs and MICs do support CFM on untagged and tagged aggregated Ethernet logical interfaces.Starting in Junos OS Release 12.3, CFM does not support Multichassis Link Aggregation (MC-LAG). Do not configure the **mc-ae** statement when you configure CFM.

Starting in Junos OS Release 11.3, on T Series and M320 routers, CFM is not supported on interfaces configured with CCC encapsulation. If you configure CFM, the system displays the following message: "**MEPs cannot be configured on ccc interface on this platform**".

Network entities such as operators, providers, and customers may be part of different administrative domains. Each administrative domain is mapped into one maintenance domain. Maintenance domains are configured with different level values to keep them separate. Each domain provides enough information for the entities to perform their own management, perform end-to-end monitoring, and still avoid security breaches.

Starting in Junos OS Release 17.4, you can enable support for IEEE 802.1ag CFM on pseudowire service interfaces by configuring maintenance intermediate points (MIPs) on the pseudowire service interfaces. Pseudowire service interfaces support configuring of subscriber interfaces over MPLS pseudowire termination. Termination of subscriber interfaces over PW enables network operators to extend their MPLS domain from the Access/Aggregation network to the service edge and use uniform MPLS label provisioning for a larger portion of their network.

> **NOTE:** The CFM MIP session is supported only on the pseudowire services interface and not on the pseudowire services tunnel interface.

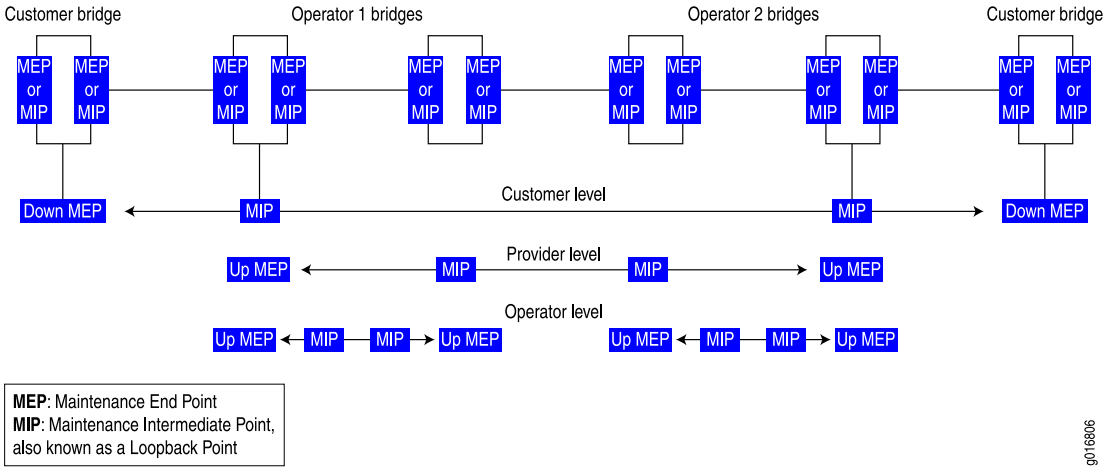
IEEE 802.1ag OAM supports graceful Routing Engine switchover (GRES). IEEE 802.1ag OAM is supported on untagged, single tagged, and stacked VLAN interfaces.

On EX Series switches, to use the CFM feature, you must first add the CFM to basic Junos OS by installing an enhanced feature license (EFL). See *Licenses for EX Series* for more details.

Connectivity Fault Management Key Elements

Figure 1 on page 27 shows the relationships among the customer, provider, and operator Ethernet bridges, maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs).

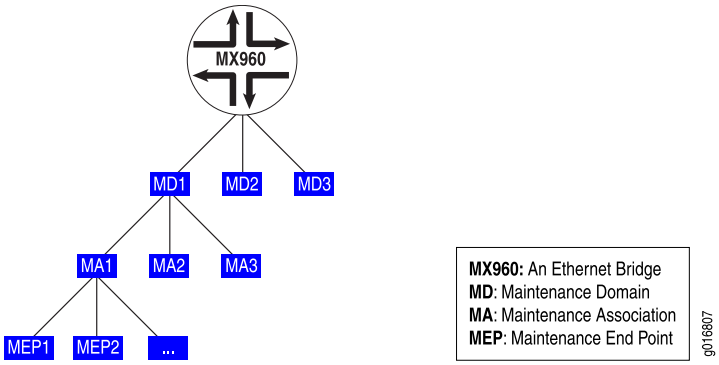
Figure 1: Relationship Among MEPs, MIPs, and Maintenance Domain Levels



> **NOTE:** On ACX Series routers, the maintenance intermediate points (MIP) are supported only on the ACX5048 and ACX5096 routers.

A maintenance association is a set of MEPs configured with the same maintenance association identifier and maintenance domain level. Figure 2 on page 27 shows the hierarchical relationships between the Ethernet bridge, maintenance domains, maintenance associations, and MEPs.

Figure 2: Relationship Among Bridges, Maintenance Domains, Maintenance Associations, and MEPs



Best Practices for Configuring 802.1ag Ethernet OAM for VPLS

BEST PRACTICE: The logical interfaces in a VPLS routing instance may have the same or different VLAN configurations. VLAN normalization is required to switch packets correctly among these interfaces. VLAN normalization is effectively VLAN translation wherein the VLAN tags of the received packet need to be translated if they are different than the normalized VLAN tags.

For MX Series routers, the normalized VLAN is specified using one of the following configuration statements in the VPLS routing instance:

- **vlan-id *vlan-number***
- **vlan-id none**
- **vlan-tags outer *outer-vlan-number* inner *inner-vlan-number***

You must configure **vlan-maps** explicitly on all interfaces belonging to the routing instance.

The following forwarding path considerations must be observed:

- Packet receive path:
  - This is the forwarding path for packets received on the interfaces.
  - 802.1ag Ethernet OAM for VPLS uses implicit interface filters and forwarding table filters to flood, accept, and drop the CFM packets.
- Packet transmit path:
  - The JUNOS Software uses the router's hardware-based forwarding for CPU-generated packets.
  - For Down MEPs, the packets are transmitted on the interface on which the MEP is configured.
  - In MX series routers, for Up MEPs, the packet must be flooded to other interfaces in the VPLS routing instance. The router creates a flood route tied to a flood next hop (with all interfaces to flood) and then sources the packet to be forwarded with this flood route.
  - The router also uses implicit-based forwarding for CPU generated packets. The result is for the flood next hop tied to the flood route to be tied to the filter term. The filter term uses match criteria to correctly identify the host- generated packets.

SEE ALSO

connectivity-fault-management

Configuring Port Status TLV and Interface Status TLV | **102**

Configuring MAC Flush Message Processing in CET Mode | 118

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4, you can enable support for IEEE 802.1ag CFM on pseudowire service interfaces by configuring maintenance intermediate points (MIPs) on the pseudowire service interfaces.
14.2	Starting in Junos OS Release 14.2, for CFM sessions in centralized mode, we recommend that you configure a maximum of 40 CFM sessions with continuity check message (CCM) interval of 100 milliseconds (100 ms) or a maximum of 400 CFM sessions with CCM interval of 1 second (1 s).
12.3	Starting in Junos OS Release 12.3, CFM does not support Multichassis Link Aggregation (MC-LAG). Do not configure the **mc-ae** statement when you configure CFM.
11.3	Starting in Junos OS Release 11.3, on T Series and M320 routers, CFM is not supported on interfaces configured with CCC encapsulation.
10.3	Starting in Junos OS Release 10.3, on interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers, CFM is not supported on untagged aggregated Ethernet member links. MPCs and MICs do support CFM on untagged and tagged aggregated Ethernet logical interfaces.
9.3	In Junos OS Release 9.3 and later, CFM also supports aggregated Ethernet interfaces.

RELATED DOCUMENTATION

CFM Monitoring between CE and PE Devices | 100
Configuring Continuity Check Messages | 124

Configuring Connectivity Fault Management (CFM)

IN THIS SECTION

Creating a Maintenance Domain | 31
Configuring Maintenance Intermediate Points (MIPs) | 32

- Configuring Maintenance Association Intermediate Points in ACX Series | **33**
- Creating a Maintenance Association | **37**
- Continuity Check Protocol Parameters Overview | **38**
- Configuring Continuity Check Protocol Parameters for Fault Detection | **39**
- Configuring a MEP to Generate and Respond to CFM Protocol Messages | **40**
- Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements | **44**
- Configuring Service Protection for VPWS over MPLS Using the MEP Interface | **46**
- Configuring Linktrace Protocol in CFM | **51**
- Configuring Rate Limiting of Ethernet OAM Messages | **52**
- Configuring Ethernet Local Management Interface | **55**
- Configuring a CFM Action Profile to Specify CFM Actions for CFM Events | **65**
- CFM Action Profile to Bring Down a Group of Logical Interfaces Overview | **66**
- Configuring a CFM Action Profile to Bring Down a Group of Logical Interfaces | **67**
- Enabling Enhanced Connectivity Fault Management Mode | **71**
- Configuring M120 and MX Series Routers for CCC Encapsulated Packets | **73**
- Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades | **75**
- Configuring Unified ISSU for 802.1ag CFM | **76**
- Junos OS Support for Performance Monitoring Compliant with Technical Specification MEF 36 | **79**
- Damping CFM performance Monitoring Traps and Notifications to Prevent Congestion of The NMS | **81**
- Example: Configuring Ethernet CFM on Physical Interfaces | **81**
- Example: Configuring Ethernet CFM on Bridge Connections | **84**
- Example: Configuring Ethernet CFM over VPLS | **89**

Use this topic to configure connectivity fault management features such as maintenance domains, maintenance associations, maintenance intermediate points (MIPs), and continuity check parameters. You can also use this topic to configure an action profile to specify the CFM action that must be performed when a specific CFM event occurs.

Creating a Maintenance Domain

To enable connectivity fault management (CFM) on an Ethernet interface, you must first configure a maintenance domain and specify the name of the maintenance domain. You can also specify the format of the name. For instance, if you specify the name format to be domain name service (DNS) format, you can specify the name of the maintenance domain as www.juniper.net. The default name format is ASCII character string.

> **NOTE:** For logical interfaces, the maintenance domain name must be unique across logical systems. If you configure the same maintenance domain name across logical systems, then you receive the following error message: **error: configuration check-out failed**.

During the creation of the maintenance domain, you can also specify the maintenance domain level. The maintenance domain level indicates the nesting relationship between various maintenance domains. The maintenance domain level is embedded in each of the CFM frames.

To create a maintenance domain:

1. In configuration mode, create a maintenance domain by specifying the name and the name format at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set maintenance-domain md-name name-format option
   ```

   > **NOTE:** If you configure the maintenance domain name length greater than 45 octet, then the following error message is displayed: **error: configuration check-out failed**.

2. Specify the maintenance domain level by specifying the value at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set maintenace-domain md-name level number
   ```

SEE ALSO

connectivity-fault-management

maintenance-domain | **1819**

name-format | 1826
level | 1811

Configuring Maintenance Intermediate Points (MIPs)

MX Series routers support maintenance intermediate points (MIPs) for the Ethernet OAM 802.1ag CFM protocol at a bridge-domain level. This enables you to define a maintenance domain for each default level. The MIPs names are created as **default-*level-number*** at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain]** hierarchy level. Use the **bridge-domain**, **instance**, **virtual-switch**, and **mip-half-function** MIP options to specify the MIP configuration.

Use the **show oam ethernet connectivity-fault-management mip (bridge-domain | instance-name | interface-name)** command to display the MIP configurations.

To configure the maintenance intermediate point (MIP):

1. Configure a bridge domain under a user-defined virtual switch by specifying the **virtual-switch** statement and the name of the user-defined virtual switch, at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* default-*x*]** hierarchy level.

   NOTE: A bridge domain must be specified by name only if it is configured by including the **vlan-id** statement under the **virtual-switch** statement. If a bridge domain is configured with a range of VLAN IDs, then the VLAN IDs must be explicitly listed after the bridge domain name.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name default-x]
   user@host# set virtual-switch virtual-switch-name bridge-domain bridge-domain-name vlan-id value
   ```

   NOTE: You can also configure the bridge domain for the default virtual switch by including the **bridge-domain** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]** hierarchy level.

2. Configure the VPLS routing instance for the default maintenance domain.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
   user@host# set instance instance-name
   ```

3. Configure the maintenance intermediate point (MIP) half function to divide the MIP fuctionality into two unidirectional segments to improve network coverage by increasing the number of MIPs that are monitored. The MIP half function also responds to loop-back and link-trace messages to identify faults.

   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 be the same.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* default- *x*]
   user@host# set mip-half-function (none | default | explicit)

SEE ALSO

bridge-domain

connectivity-fault-management

instance | **1800**

mip-half-function | **1825**

virtual-switch

Configuring Maintenance Association Intermediate Points in ACX Series

IN THIS SECTION

- Configuring the Maintenance Domain Bridge Domain | **34**
- Configuring the Maintenance Domain MIP Half Function | **35**
- Configuring the Maintenance Association Intermediate Points with Bridge Domain | **35**
- Configuring the Maintenance Association Intermediate Points with Circuit Cross-Connect | **35**
- Configuring the Maintenance Association Intermediate Points with Bridge Domain when Maintenance Association End Point is Configured | **36**
- Configuring the Maintenance Intermediate Points with Circuit Cross-Connect when Maintenance Association End Point is Configured | **36**

Maintenance Intermediate Point (MIP) provides monitoring capability of intermediate points for services such as Layer 2 bridging, Layer 2 circuit, and Layer 2 VPN. ACX5048 and ACX5096 routers support MIPs for the Ethernet OAM 802.1ag CFM protocol. Use the bridge-domain, interface, and mip-half-function MIP options to specify the MIP configuration.

NOTE: ACX5048 and ACX5096 routers do not support MIP configuration on VPLS services.

NOTE: ACX5448 router do not support MIP.

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 be the same.

To display MIP configurations, use the **show oam ethernet connectivity-fault-management mip (bridge-domain | instance-name | interface-name)** command.

The following MIP configurations are supported in ACX5048 and ACX5096 routers:

- MIP with with bridge domain
- MIP with circuit cross-connect (CCC)
- MIP with bridge domain when maintenance association end point is configured
- MIP with CCC when maintenance association end point is configured

The following sections describe MIP configuration:

Configuring the Maintenance Domain Bridge Domain

To configure the bridge domain, include the **vlans** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain-name*]** hierarchy level.

NOTE: The Layer 2 CLI configurations and show commands for ACX5048 and ACX5096 routers differ compared to other ACX Series routers. For more information, see *Layer 2 Next Generation Mode for ACX Series*.

Configuring the Maintenance Domain MIP Half Function

MIP Half Function (MHF) divides MIP functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loopback and linktrace messages to help isolate faults.

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 be the same. To configure the MIP half function, include the **mip-half-function** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain-name*]** hierarchy level.

Configuring the Maintenance Association Intermediate Points with Bridge Domain

In ACX5048 and ACX5096 routers, you can configure the MIP with bridge domain. The following is a sample to configure the MIP with bridge domain:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain default-6 {
                vlan bd1;
                mip-half-function default;
            }
        }
    }
}
```

Configuring the Maintenance Association Intermediate Points with Circuit Cross-Connect

In ACX5048 and ACX5096 routers, you can configure the MIP with circuit cross-connect (CCC). The following is a sample to configure the MIP with CCC:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain default-6 {
                interface xe-0/0/42.0;
                mip-half-function default;
            }
        }
    }
}
```

Configuring the Maintenance Association Intermediate Points with Bridge Domain when Maintenance Association End Point is Configured

In ACX5048 and ACX5096 routers, you can configure the MIP with bridge domain when a maintenance association end point (MEP) is configured. The following is a sample to configure the MIP with bridge domain when MEP is configured:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md2 {
                level 5;
                mip-half-function default;
                maintenance-association ma2 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 222 {
                        interface xe-0/0/42.0;
                        direction up;
                    }
                }
            }
        }
    }
}
```

Configuring the Maintenance Intermediate Points with Circuit Cross-Connect when Maintenance Association End Point is Configured

In ACX5048 and ACX5096 routers, you can configure the MIP with circuit cross-connect (CCC) when a maintenance association end point (MEP) is configured. The following is a sample to configure the MIP with CCC when MEP is configured:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md2 {
                level 5;
                mip-half-function default;
                maintenance-association ma2 {
                    continuity-check {
                        interval 1s;
                    }
```

```
            mep 222 {
              interface xe-0/0/42.0;
              direction up;
            }
          }
        }
      }
    }
  }
```

SEE ALSO

- *bridge-domain*
- *connectivity-fault-management*
- instance | **1800**
- mip-half-function | **1825**

Creating a Maintenance Association

To create a maintenance association, include the **maintenance-association *ma-name*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]** hierarchy level.

Maintenance association names can be in one of the following formats:

- As a plain ASCII character string
- As the VLAN identifier of the VLAN you primarily associate with the maintenance association
- As a two-octet identifier in the range from 0 through 65,535
- As a name in the format specified by RFC 2685

The default short name format is an ASCII character string.

To configure the maintenance association short name format, include the **short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id)** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name*]** hierarchy level.

SEE ALSO

connectivity-fault-management

name-format | **1826**

short-name-format | **1844**

Continuity Check Protocol Parameters Overview

The continuity check protocol is used for fault detection by maintenance end points (MEPs) within a maintenance association. The MEP periodically sends continuity check multicast messages. The continuity check protocol packets use the ethertype value 0x8902 and the multicast destination MAC address 01:80:c2:00:00:32.

The following list describes the continuity check protocol parameters you can configure:

- **interval**—Frequency of the continuity check messages (CCM) i.e time between the transmission of the CCM messages. You can specify 10 minutes (**10m**), 1 minute (**1m**), 10 seconds (**10s**), 1 second (**1s**), 100 milliseconds (**100ms**), or 10 milliseconds (**10ms**). The default value is 1 minute. For instance, if you specify the interval as 1 minute, the MEP sends the continuity check messages every minute to the receiving MEP.

  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 only disable PPM 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.

  Continuity check interval of 10 milliseconds is not supported for CFM sessions over a label-switched interface (LSI).

- **hold-interval**—Frequency at which the MEP database can be flushed, if no updates occur. Receiving MEPs use the continuity check messages to build a MEP database of all MEPs in the maintenance association. The frequency is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes.

  NOTE: Hold timer based flushing is applicable only for autodiscovered remote MEPs and not for statically configured remote MEPs.

  The hold interval logic runs a polling timer per CFM session level (not per remote MEP level) where the polling timer duration is equal to the configured hold time. When the polling timer expires, it deletes all the autodiscovered remote MEP entries which have been in the failed state for a time period equal to or greater than the configured hold time. If the remote MEP completes the hold time duration in the

failed state, then flushing will not occur until the next polling timer expires. Hence remote MEP flushing may not happen exactly at the configured hold time.

- **loss-threshold**—Number of continuity check messages that can be lost before the router marks the MEP as down. The value can be from 3 to 256 protocol data units (PDUs). The default value is 3 PDUs.

SEE ALSO

hold-interval | 1799

interval | 1808

loss-threshold | 1815

Configuring Continuity Check Protocol Parameters for Fault Detection

The continuity check protocol is used for fault detection by a maintenance association end point (MEP) within a maintenance association. A MEP periodically generates and responds to continuity check multicast messages. The continuity check protocol packets use the ethertype value 0x8902 and the multicast destination MAC address 01:80:c2:00:00:32. The receiving MEPs use the continuity check messages (CCMs) to build a MEP database of all MEPs in the maintenance association.

To configure continuity check protocol parameters:

1. Specify the time to wait in minutes before flushing the MEP database, if no updates occur, with a value from 1 minute through 30,240 minutes. The default value is 10 minutes.

   NOTE: Flushing based on the hold timer is applicable only for autodiscovered remote MEPs and not for statically configured remote MEPs.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
     maintenance-association ma-name  continuity-check]
   user@host# set hold-interval minutes
   ```

2. Specify the time to wait (duration) between the transmissions of CCMs. The duration can be one of the following values: 10 minutes (10m), 1 minute (1m), 10 seconds (10s), 1 second (1s), 100 milliseconds (100ms), or 10 milliseconds (10ms). The default value is 1 minute.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
     maintenance-association ma-name continuity-check]
   ```

```
user@host# set interval duration
```

3. Specify the number of continuity check messages that can be lost before the router marks the MEP as down. The value can be from 3 to 256 protocol data units (PDUs). The default value is 3 PDUs.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name continuity-check]
user@host# set loss-threshold number
```

SEE ALSO

- continuity-check | 1777
- hold-interval | 1799
- interval | 1808
- loss-threshold | 1815

Configuring a MEP to Generate and Respond to CFM Protocol Messages

IN THIS SECTION

- Configuring a Maintenance Association End Point (MEP) | 41
- Configuring a remote Maintenance Association End Point (MEP) | 43

A maintenance association end point (MEP) refers to the boundary of a domain. A MEP generates and responds to connectivity fault management (CFM) protocol messages. You can configure multiple up MEPs for a single combination of maintenance association ID and maintenance domain ID for interfaces belonging to a particular VPLS service or a bridge domain. You can configure multiple down MEPs for a single instance of maintenance domain identifier and maintenance association name to monitor services provided by Virtual Private LAN service (VPLS), bridge domain, circuit cross-connect (CCC), or IPv4 domains.

For layer 2 VPNs routing instances (local switching) and EVPN routing instances, you can also configure multiple up MEPs for a single combination of maintenance association ID and maintenance domain ID on logical interfaces. The logical interface can be configured on different devices or on the same device. To support multiple up MEPs on two IFLs, enhanced IP network services must be configured for the chassis.

You can enable automatic discovery of a MEP. With automatic discovery a MEP is enabled to accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association. If automatic discovery is not enabled, the remote MEPs must be configured. If the remote MEP is not configured, the CCMs from the remote MEP are treated as errors.

Continuity measurement is provided by an existing continuity check protocol. The continuity for every remote MEP is measured as the percentage of time that remote MEP was operationally up over the total administratively enabled time. Here, the operational uptime is the total time during which the CCM adjacency is active for a particular remote MEP and the administrative enabled time is the total time during which the local MEP is active. You can also restart the continuity measurement by clearing the currently measured operational uptime and the administrative enabled time.

Configuring a Maintenance Association End Point (MEP)

To configure a maintenance association end point:

1. Specify an ID for the MEP at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name***]. You can specify any value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-name]
user@host# set mep mep-id
```

2. Enable maintenance end point automatic discovery so the MEP can accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

3. Specify the direction in which the CCM packets are transmitted for the MEP. You can specify up or down. If you specify the direction as up, CCMs are transmitted out of every logical interface that is part of the same bridging or VPLS instance except for the interface configured on the MEP. If you specify the direction as down, CCMs are transmitted only out of the interface configured on the MEP.

> **NOTE:** Ports in the Spanning Tree Protocol (STP) blocking state do not block CFM packets destined to a down MEP. Ports in an STP blocking state without the continuity check protocol configured do block CFM packets.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set direction down
```

NOTE: Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs. For all other interfaces on MX Series routers and on all other routers and switches, you must continue to configure the **no-control-word** statement at the **[edit routing-instances *routing-instance-name* protocols l2vpn]** or **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]** hierarchy level when you configure CFM MEPs. Otherwise, the CFM packets are not transmitted, and the **show oam ethernet connectivity-fault-management mep-database** command does not display any remote MEPs.

4. Specify the interface to which the MEP is attached. It can be a physical interface, logical interface, or trunk interface. On MX Series routers, the MEP can be attached to a specific VLAN of a trunk interface.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set interface interface-name
```

5. Specify the IEEE 802.1 priority bits that are used by continuity check and link trace messages. You can specify a value from through 7 as the priority.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set priority number
```

6. Specify the lowest priority defect that generates a fault alarm whenever CFM detects a defect. Possible values include: all -defects, err-xcon, mac-rem-err-xcon, no-defect, rem-err-xcon, and xcon.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set lowest-priority-defect mac-rem-err-xcon
```

7. Specify the ID of the remote MEP at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id***]. You can specify any value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-namemep mep-id]
user@host# set remote-mep mep-id
```

SEE ALSO

priority | **1836**

Configuring a remote Maintenance Association End Point (MEP)

To configure a remote maintenance association end point:

1. Configure the remote MEP by specifying the MEP ID at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id***]. You can specify any value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-namemep mep-id]
user@host# edit remote-mep mep-id
```

2. Specify the name of the action profile to be used for the remote MEP by including the **action-profile *profile-name*** statement at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id* remote-mep *remote-mep-id***]. The profile must be defined at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-namemep mep-id remote-mep remote-mep-id]
user@host# set action-profile profile-name
```

3. Configure the remote MEP to detect initial loss of connectivity. By default, the MEP does not generate loss-of-continuity (LOC) defect messages. When you configure the **detect-loc** statement, a loss-of-continuity (LOC) defect is detected if no continuity check message is received from the remote MEP within a period equal to 3.5 times the continuity check interval configured for the maintenance association. If a LOC defect is detected, a syslog error message is generated.

NOTE: When you configure connectivity-fault management (CFM) along with **detect-loc**, any **action-profile** configured to bring down the interface is executed if continuity check message is not received . However, the **action-profile** is not executed if you have not configured **detect-loc** and continuity check message is not received.

[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name*mep *mep-id* remote-mep *remote-mep-id*]
user@host# set detect-loc

SEE ALSO

remote-mep | **1842**

SEE ALSO

action-profile | **1759**

auto-discovery | **1763**

connectivity-fault-management

detect-loc | **1786**

direction | **1788**

lowest-priority-defect | **1816**

Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging Service Level Agreements (SLAs). By default, Ethernet frame delay measurement uses software for timestamping and delay calculations. You can optionally use hardware timing to assist in this process and increase the accuracy of the delay measurement results. This assistance is available on the reception path.

Before you can perform Ethernet frame delay measurements on MX Series routers, you must have done the following:

- Configured Ethernet OAM and CFM correctly
- Prepared the measurement between two compatibly configured MX Series routers

- Enabled the distributed periodic packet management daemon (ppmd)
- Avoided trying to perform Ethernet frame delay measurement on aggregated Ethernet or pseudowire interfaces, which are not supported
- Made sure the hardware-assisted timestamping is supported if that feature is configured

At the end of this configuration, you create two MX Series routers that can perform and display Ethernet frame delay measurements on Ethernet interfaces using optional hardware timestamping. By default, Ethernet frame delay measurement uses software for timestamping and delay calculations. You can optionally use hardware timing to assist in this process and increase the accuracy of the delay measurement results. This assistance is available on the reception path.

To configure hardware-assisted timestamping:

1. To enable Ethernet frame delay measurement hardware assistance on the reception path, include the **hardware-assisted-timestamping** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level:

```
[edit]
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    hardware-assisted-timestamping; # Enable timestamping in hardware.
                }
            }
        }
    }
```

2. Ethernet frame delay measurement requires that distributed PPMD is enabled. Before you can gather statistics for Ethernet frame delay measurement, you must make sure that PPMD is configured properly. Without distributed PPMD, delay measurement results are not valid.

   To perform Ethernet frame delay measurement, make sure that the following configuration statement is *NOT* present:

```
[edit routing-options]
ppm {
    no-delegate-processing; # This turns distributed PPMD OFF.
}
```

SEE ALSO

Ethernet Frame Delay Measurements Overview | 166

Triggering an Ethernet Frame Delay Measurements Session | 199

Viewing Ethernet Frame Delay Measurements Statistics | 217

Example: Configuring One-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | 204

Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | 210

Configuring ETH-DM with Untagged Interfaces

Configuring Service Protection for VPWS over MPLS Using the MEP Interface

You can enable service protection for a virtual private wire service (VPWS) over MPLS by specifying a working path or protect path on the MEP. Service protection provides end-to-end connection protection of the working path in the event of a failure.

To configure service protection, you must create two separate transport paths—a working path and a protect path. You can specify the working path and protect path by creating two maintenance associations. To associate the maintenance association with a path, you must configure the **interface** statement for the MEP within the maintenance association and specify the path as working or protect.

NOTE: If the path is not specified, the session monitors the active path.

Table 7 on page 46 describes the available service protection options.

Table 7: Service Protection Options

Option	Description
working	Specifies the working path.
protect	Specifies the protect path.

In this configuration, we enable service protection for the VPWS service. The CCM session is configured for the working path and references the CCM session configured for the protect path using the **protect-maintenance-association** statement. The name of the protect transport path for the maintenance association is configured and associated with the maintenance association for the working path.

To configure service protection for VPWS over MPLS:

1. In configuration mode, create a maintenance domain by specifying the name and the name format at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain md-name name-format option
```

NOTE: If you configure the maintenance domain name length greater than 45 octet, then the following error message is displayed: **error: configuration check-out failed**.

2. Specify the maintenance domain level by specifying the value at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenace-domain md-name level number
```

3. Create a maintenance association for the working path by specifying the name and the short name format at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name***] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# set maintenance-association test-ma short-name-format option
```

4. Specify the maintenance association name used for connection protection and the name of the automatic-protection-switching profile (aps-profile) at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name***] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name]
user@host# set protect-maintenance-association ma-name aps-profile aps-profile-name
```

5. Specify the time to wait between transmissions of continuity check messages at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* continuity-check**] hierarchy level. The duration can be one of the following values: 10 minutes(10m), 1 minute(1m), 10 seconds(10s), 1 second(1s), 100 milliseconds(100ms), or 10 milliseconds(10ms). The default value is 1 minute.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name continuity-check]
user@host# set interval option
```

6. Specify an ID for the MEP at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name***]. You can specify any value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name]
user@host# set mep mep-id
```

7. Enable maintenance end point automatic discovery so the MEP can accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

8. Specify the direction in which the CCM packets are transmitted for the MEP. You can specify up or down. If you specify the direction as up, CCMs are transmitted out of every logical interface that is part of the same bridging or VPLS instance except for the interface configured on the MEP. If you specify the direction as down, CCMs are transmitted only out of the interface configured on the MEP.

> **NOTE:** Ports in the Spanning Tree Protocol (STP) blocking state do not block CFM packets destined to a down MEP. Ports in an STP blocking state without the continuity check protocol configured do block CFM packets.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set direction down
```

> **NOTE:** Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs. For all other interfaces on MX Series routers and on all other routers and switches, you must continue to configure the **no-control-word** statement at the **[edit routing-instances *routing-instance-name* protocols l2vpn]** or **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]** hierarchy level when you configure CFM MEPs. Otherwise, the CFM packets are not transmitted, and the **show oam ethernet connectivity-fault-management mep-database** command does not display any remote MEPs.

9. Specify the interface to which the MEP is attached. It can be a physical interface, logical interface, or trunk interface. On MX Series routers, the MEP can be attached to a specific VLAN of a trunk interface. Also, specify the transport path as working.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set interface interface-name working
```

10. Create a maintenance association for the protection path by specifying the name and the short name format at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name***] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# set maintenance-association ma-name short-name-format option
```

11. Specify the time to wait between transmissions of continuity check messages at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* continuity-check**] hierarchy level. The duration can be one of the following values: 10 minutes(10m), 1 minute(1m), 10 seconds(10s), 1 second(1s), 100 milliseconds(100ms), or 10 milliseconds(10ms). The default value is 1 minute.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name continuity-check]
user@host# set interval option
```

12. Specify an ID for the MEP at the [**edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name***]. You can specify any value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name]
user@host# set mep mep-id
```

13. Enable maintenance end point automatic discovery so the MEP can accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

14. Specify the direction in which the CCM packets are transmitted for the MEP. You can specify up or down. If you specify the direction as up, CCMs are transmitted out of every logical interface that is part of the same bridging or VPLS instance except for the interface configured on the MEP. If you specify the direction as down, CCMs are transmitted only out of the interface configured on the MEP.

    NOTE: Ports in the Spanning Tree Protocol (STP) blocking state do not block CFM packets destined to a down MEP. Ports in an STP blocking state without the continuity check protocol configured do block CFM packets.

    ```
    [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
      maintenance-association ma-name mep mep-id]
    user@host# set direction down
    ```

    NOTE: Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs. For all other interfaces on MX Series routers and on all other routers and switches, you must continue to configure the **no-control-word** statement at the **[edit routing-instances *routing-instance-name* protocols l2vpn]** or **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]** hierarchy level when you configure CFM MEPs. Otherwise, the CFM packets are not transmitted, and the **show oam ethernet connectivity-fault-management mep-database** command does not display any remote MEPs.

15. Specify the interface to which the MEP is attached. It can be a physical interface, logical interface, or trunk interface. On MX Series routers, the MEP can be attached to a specific VLAN of a trunk interface. Also, specify the transport path as working.

    ```
    [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
      maintenance-association ma-name mep mep-id]
    user@host# set interface interface-name protect
    ```

SEE ALSO

auto-discovery | **1763**

interval | **1806**

name-format | 1826

protect-maintenance-association | 1838

short-name-format | 1844

Configuring Linktrace Protocol in CFM

The linktrace protocol is used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the **traceroute** command to verify the path between a pair of MEPs under the same maintenance association. Linktrace messages can also be used to verify the path between an MEP and an MIP under the same maintenance domain. The linktrace protocol enables you to configure the time to wait for a response. If no response is received for a linktrace request message, the request and response entries are deleted after the interval expires. You can also configure the number of linktrace reply entries to be stored for the corresponding linktrace request.

The operation of IEEE 802.1ag linktrace request and response messages is similar to the operation of Layer 3 **traceroute** commands. For more information about the **traceroute** command, see the *Junos OS Administration Library*.

To configure the linktrace protocol:

1. Configure the time to wait for a linktrace response at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level. You can specify the value in minutes or seconds. The default value is 10 minutes.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set linktrace age time
   ```

2. Configure the number of linktrace reply entries to be stored per linktrace request. You can specify a value from 1 through 500. The default value is 100.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set linktrace path-database-sizepath-database-size
   ```

SEE ALSO

age | 1857

path-database-size | 1828

connectivity-fault-management

Configuring Rate Limiting of Ethernet OAM Messages

The M320 with Enhanced III FPC, M120, M7i, M10 with CFEB, and MX Series routers support rate limiting of Ethernet OAM messages. Depending on the connectivity fault management (CFM) configuration, CFM packets are discarded, sent to the CPU for processing, or flooded to other bridge interfaces. This feature allows the router to intercept incoming CFM packets for prevention of DoS attacks.

You can apply rate limiting of Ethernet OAM messages at either of two CFM policing levels, as follows:

- Global-level CFM policing—uses a policer at the global level to police the CFM traffic belonging to all the sessions.
- Session-level CFM policing—uses a policer created to police the CFM traffic belonging to one session.

To configure global-level CFM policing, include the **policer** statement and its options at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

To configure session-level CFM policing, include the **policer** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* level *number* maintenance-association *ma-name*]** hierarchy level.

The following example shows a CFM policer used for rate-limiting CFM:

```
[edit]
firewall {
    policer cfm-policer {
        if-exceeding {
            bandwidth-limit 8k;
            burst-size-limit 2k;
        }
        then discard;
    }
}
```

Case 1: Global-Level CFM Policing

This example shows a global level policer, at the CFM level, for rate-limiting CFM. The **continuity-check *cfm-policer*** statement at the global **[edit protocols oam ethernet connectivity-fault-management policer]** hierarchy level specifies the policer to use for policing all continuity check packets of the CFM traffic belonging to all sessions. The **other *cfm-policer1*** statement at the **[edit protocols oam ethernet connectivity-fault-management policer]** hierarchy level specifies the policer to use for policing all non-continuity check packets of the CFM traffic belonging to all sessions. The **all *cfm-policer2*** statement specifies to police all CFM packets with the specified policer *cfm-policer2*. If the **all *policer-name*** option is used, then the user cannot specify the previous **continuity-check** and **other** options.

```
[edit protocols oam ethernet]
connectivity-fault-management {
   policer {
      continuity-check cfm-policer;
      other cfm-policer1 ;
      all cfm-policer2;
      }
   }
```

Case 2: Session-Level CFM Policing

This example shows a session-level CFM policer used for rate-limiting CFM. The **policer** statement at the session **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name*]** hierarchy level specifies the policer to use for policing only continuity check packets of the CFM traffic belonging to the specified session. The **other *cfm-policer1*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name*]** hierarchy level specifies the policer to use for policing all non-continuity check packets of the CFM traffic belonging to this session only. The **all *cfm-policer2*** statement specifies to police all CFM packets with the specified policer *cfm-policer2*. If the **all *policer-name*** option is used, then the user cannot specify the previous **continuity-check** and **other** options.

```
[edit protocols oam ethernet]
connectivity-fault-management {
   maintenance-domain md {
      level number;
      maintenance-association ma {
         continuity-check {
            interval 1s;
         }
         policer {
```

```
            continuity-check cfm-policer;
            other cfm-policer1;
            all cfm-policer2;
            }
        }
        mep 1 {
            interface ge-3/3/0.0;
            direction up;
            auto-discovery;
        }
    }
}
```

In the case of global CFM policing, the same policer is shared across multiple CFM sessions. In per-session CFM policing, a separate policer must be created to rate-limit packets specific to that session.

NOTE:
Service-level policer configuration for any two CFM sessions on the same interface at different levels must satisfy the following constraints if the direction of the sessions is the same:

- If one session is configured with **policer all**, then the other session cannot have a **policer all** or **policer other** configuration.
- If one session is configured with **policer other**, then the other session cannot have a **policer all** or **policer other** configuration.

A commit error will occur if such a configuration is committed.

NOTE: Policers with PBB and MIPs are not supported.

SEE ALSO

policer | 1832

policer | 1831

show oam ethernet connectivity-fault-management policer | 2782

clear oam ethernet connectivity-fault-management policer | 2645

Configuring Ethernet Local Management Interface

IN THIS SECTION

- Ethernet Local Management Interface Overview | 55
- Configuring the Ethernet Local Management Interface | 57
- Example E-LMI Configuration | 59

Ethernet Local Management Interface Overview

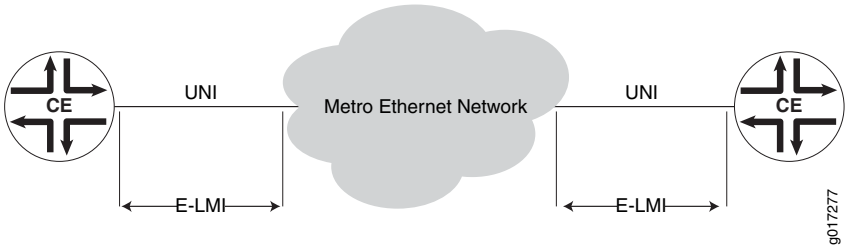
Gigabit Ethernet (**ge**), 10-Gigabit Ethernet (**xe**), and Aggregated Ethernet (**ae**) interfaces support the Ethernet Local Management Interface (E-LMI).

> **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.

The E-LMI specification is available at the Metro Ethernet Forum. E-LMI procedures and protocols are used for enabling automatic configuration of the customer edge (CE) to support Metro Ethernet services. The E-LMI protocol also provides user-to-network interface (UNI) and Ethernet virtual connection (EVC) status information to the CE. The UNI and EVC information enables automatic configuration of CE operation based on the Metro Ethernet configuration.

The E-LMI protocol operates between the CE device and the provider edge (PE) device. It runs only on the PE-CE link and notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port. The scope of the E-LMI protocol is shown in Figure 3 on page 55.

Figure 3: Scope of the E-LMI Protocol



The E-LMI implementation on ACX and MX Series routers includes only the PE side of the E-LMI protocol.

E-LMI interoperates with an OAM protocol, such as Connectivity Fault Management (CFM), that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level (UNI-N

to UNI-N with up MEPs at the UNI). E-LMI relies on the CFM for end-to-end status of EVCs across CFM domains (SVLAN domain or VPLS).

The E-LMI protocol relays the following information:

- Notification to the CE of the addition/deletion of an EVC (active, not active, or partially active)
- Notification to the CE of the availability state of a configured EVC
- Communication of UNI and EVC attributes to the CE:
  - UNI attributes:
    - UNI identifier (a user-configured name for UNI)
    - CE-VLAN ID/EVC map type (all-to-one bundling, service multiplexing with bundling, or no bundling)
    - Bandwidth profile is not supported (including the following features):
      - CM (coupling mode)
      - CF (color flag)
      - CIR (committed Information rate)
      - CBR (committed burst size)
      - EIR (excess information rate)
      - EBS (excess burst size)
  - EVC attributes:
    - EVC reference ID
    - EVC status type (active, not active, or partially active)
    - EVC type (point-to-point or multipoint-to-multipoint)
    - EVC ID (a user-configured name for EVC)
    - Bandwidth profile (not supported)
  - CE-VLAN ID/EVC map

E-LMI on MX Series routers supports the following EVC types:

- Q-in-Q SVLAN (point-to-point or multipoint-to-multipoint)—Requires an end-to-end CFM session between UNI-Ns to monitor the EVS status.
- VPLS (BGP or LDP) (point-to-point or multipoint-to-multipoint)—Either VPLS pseudowire status or end-to-end CFM sessions between UNI-Ns can be used to monitor EVC status.
- L2 circuit/L2VPN (point-to-point)—Either VPLS pseudowire status or end-to-end CFM sessions between UNI-Ns can be used to monitor EVC status.

> **NOTE:** **l2-circuit** and **l2vpn** are not supported.

The E-LMI protocol on ACX Series routers supports Layer 2 circuit and Layer 2 VPN EVC types and enables link-loss forwarding for pseudowire (Layer 2 circuit and Layer 2 VPN) services as follows:

- Interworking between the connectivity fault management (CFM) protocol and the E-LMI protocol for Layer 2 circuit and Layer 2 VPN.
  - End-to-end CFM session between UNIs to monitor EVC status.
  - In the case of pseudowire redundancy, CFM can be used to monitor active and backup pseudowire sessions. The EVC status is declared as down to CE devices only when both the active and backup pseudowire sessions go down.
- Interworking between remote defect indication (RDI) and E-LMI for Layer 2 circuit and Layer 2 VPN.
  - If a maintenance association end point (MEP) receives an RDI bit set in a continuity check message (CCM) frame, and if RDI fault detection is enabled in the EVC configuration at **[edit protocols oam ethernet evcs *evc-id* evc-protocol *cfm* management-domain *name* management-association *name* faults rdi]**, then the pseudowire is declared as down to CE routers through E-LMI.
- If an end-to-end CFM session does not exist between UNIs, the pseudowire (Layer 2 circuit or Layer 2 VPN) up and down state triggers an asynchronous EVC state change message to CE routers through E-LMI.

> **NOTE:** ACX Series routers do not support E-LMI for Layer 2 services (bridging).

Configuring the Ethernet Local Management Interface

IN THIS SECTION

- Configuring an OAM Protocol (CFM) | **58**
- Assigning the OAM Protocol to an EVC | **58**
- Enabling E-LMI on an Interface and Mapping CE VLAN IDs to an EVC | **58**

To configure E-LMI, perform the following steps:

Configuring an OAM Protocol (CFM)

For information on configuring the OAM protocol (CFM), see "IEEE 802.1ag OAM Connectivity Fault Management Overview" on page 24.

Assigning the OAM Protocol to an EVC

To configure an EVC, you must specify a name for the EVC using the **evcs*evc-id*** statement at the **[edit protocols oam ethernet]** hierarchy level. You can set the EVC protocol for monitoring EVC statistics to **cfm** or **vpls** using the **evc-protocol** statement and its options at the **[edit protocols oam ethernet evcs]** hierarchy level.

You can set the number of remote UNIs in the EVC using the **remote-uni-count *number*** statement at the **[edit protocols oam ethernet evcs evcs-protocol]** hierarchy level. The **remote-uni-count** defaults to 1. Configuring a value greater than 1 makes the EVC multipoint-to-multipoint. If you enter a value greater than the actual number of endpoints, the EVC status will display as partially active even if all endpoints are up. If you enter a **remote-uni-count** less than the actual number of endpoints, the status will display as active, even if all endpoints are not up.

You can configure an EVC by including the **evcs** statement at the **[edit protocols oam ethernet]** hierarchy level:

```
[edit protocols oam ethernet]
evcs evc-id {
   evc-protocol (cfm (management-domain name management-association name ) | vpls (routing-instance name))
      {
      remote-uni-count <number>; # Optional, defaults to 1
      multipoint-to-multipoint;
         # Optional, defaults to point-to-point if remote-uni-count is 1
   }
}
```

Enabling E-LMI on an Interface and Mapping CE VLAN IDs to an EVC

To configure E-LMI, include the **lmi** statement at the **[edit protocols oam ethernet]** hierarchy level:

```
[edit protocols oam ethernet]
lmi {
   polling-verification-timer value;
      # Polling verification timer (T392), defaults to 15 seconds
   status-counter count; # Status counter (N393), defaults to 4
   interface name {
      evc evc-id {
         default-evc;
         vlan-list [ vlan-ids ];
      }
      evc-map-type (all-to-one-bundling | bundling | service-multiplexing);
```

```
        polling-verification-time value; # Optional, defaults to global value
        status-counter count; # Optional, defaults to global value
        uni-id value; # Optional, defaults to interface-name
    }
}
```

You can set the status counter to count consecutive errors using the **status-counter *count*** statement at the **[edit protocols oam ethernet lmi]** hierarchy level. The status counter is used to determine if E-LMI is operational or not. The default value is 4.

You can set the **polling-verification-timer *value*** statement at the **[edit protocols oam ethernet lmi]** hierarchy level. The default value is 15 seconds.

You can enable an interface and set its options for use with E-LMI using the **interface *name*** statement at the **[edit protocols oam ethernet lmi]** hierarchy level. Only **ge**, **xe**, and **ae** interfaces are supported. You can use the interface **uni-id** option to specify a name for the UNI. If **uni-id** is not configured, it defaults to the name variable of **interface *name***.

You can specify the CE-VLAN ID/EVC map type using the **evc-map-type type** interface option. The options are **all-to-one-bundling**, **bundling**, or **service-multiplexing**. Service multiplexing is with no bundling. The default type is **all-to-one-bundling**.

To specify the EVC that an interface uses, use the **evc *evc-id*** statement at the **[edit protocols oam ethernet lmi interface *name*]** hierarchy level. You can specify an interface as the default EVC interface using the **default-evc** statement at the **[edit protocols oam ethernet lmi interface *name* evc *evc-id*]** hierarchy level. All VIDs that are not mapped to any other EVCs are mapped to this EVC. Only one EVC can be configured as the default.

You can map a list of VLANs to an EVC using the **vlan-list *vlan-id-list*** statement at the **[edit protocols oam ethernet lmi interface *name* evc *evc-id*]** hierarchy level.

Example E-LMI Configuration

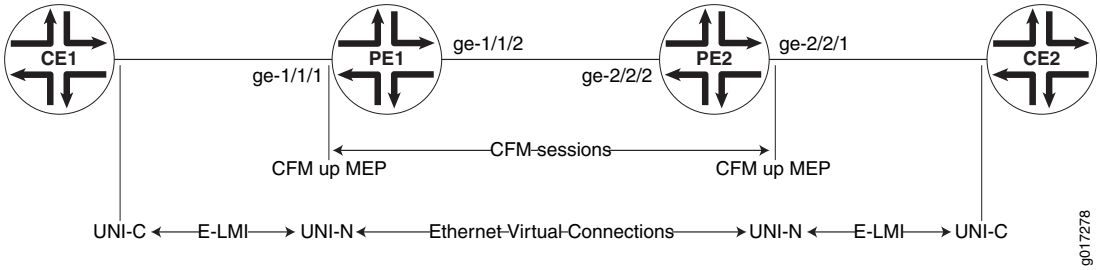
IN THIS SECTION

- Example Topology | **60**
- Configuring PE1 | **60**
- Configuring PE2 | **62**
- Configuring Two UNIs Sharing the Same EVC | **64**

Example Topology

Figure 4 on page 60 illustrates the E-LMI configuration for a point-to-point EVC (SVLAN) monitored by CFM. In this example, VLANs 1 through 2048 are mapped to **evc1** (SVLAN 100) and 2049 through 4096 are mapped to **evc2** (SVLAN 200). Two CFM sessions are created to monitor these EVCs.

Figure 4: E-LMI Configuration for a Point-to-Point EVC (SVLAN) Monitored by CFM



Configuring PE1

```
[edit]
interfaces {
   ge-1/1/1 {
      unit 0 {
         family bridge {
            interface-mode trunk;
            vlan-id-list 1-2048;
         }
      }
      unit 1 {
         family bridge {
            interface-mode trunk;
            vlan-id-list 2049-4096;
         }
      }
   }
   ge-1/1/2 {
      unit 0 {
         vlan-id 100;
         family bridge {
            interface-mode trunk;
            inner-vlan-id-list 1-2048;
         }
      }
      unit 1 {
         vlan-id 200;
         family bridge {
            interface-mode trunk;
```

```
            inner-vlan-id-list 2049-4096;
          }
        }
      }
    }
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 0;
                    maintenance-association 1 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-1/1/1.0 vlan 1;
                        }
                    }
                    maintenance-association 2049 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-1/1/1.1 vlan 2049;
                        }
                    }
                }
            }
            evcs {
                evc1 {
                    evc-protocol cfm management-domain md management-association 1;
                    remote-uni-count 1;
                }
                evc2 {
                    evc-protocol cfm management-domain md management-association 2049;
                    remote-uni-count 1;
                }
            }
            lmi {
                interface ge-1/1/1 {
                    evc evc1 {
                        vlan-list 1-2048;
                    }
                    evc evc2 {
                        vlan-list 2049-4096;
```

```
            }
            evc-map-type bundling;
            uni-id uni-ce1;
          }
        }
      }
    }
}
```

Configuring PE2

```
[edit]
interfaces {
    ge-2/2/1 {
        unit 0 {
            family bridge {
                interface-mode trunk;
                vlan-id-list 1-2048;
            }
        }
        unit 1 {
            family bridge {
                interface-mode trunk;
                vlan-id-list 2049-4096;
            }
        }
    }
    ge-2/2/2 {
        unit 0 {
            vlan-id 100;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 1-2048;
            }
        }
        unit 1 {
            vlan-id 200;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 2049-4095;
            }
        }
    }
}
```

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 0;
                    maintenance-association 1 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.0 vlan 1;
                        }
                    }
                    maintenance-association 2049 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.1 vlan 2049;
                        }
                    }
                }
            }
            evcs {
                evc1 {
                    evc-protocol cfm management-domain md management-association 1;
                    remote-uni-count 1;
                }
                evc2 {
                    evc-protocol cfm management-domain md management-association 2049;
                    uni-count 2;
                }
            }
            lmi {
                interface ge-2/2/1 {
                    evc evc1 {
                        vlan-list 1-2048;
                    }
                    evc evc2 {
                        vlan-list 2049-4095;
                    }
                    evc-map-type bundling;
                    uni-id uni-ce2;
                }
            }
```

```
      }
    }
  }
```

Configuring Two UNIs Sharing the Same EVC

```
[edit protocols]
oam {
   ethernet {
      connectivity-fault-management { ...}
      evcs {
         evc1 {
            evc-protocol cfm management-domain md management-association 1;
            remote-uni-count 1;
         }
      }
      lmi {
         interface ge-2/2/1 {
            evc evc1 {
               vlan-list 0-4095;
            }
            evc-map-type all-to-one-bundling;
            uni-id uni-ce1;
         }
         interface ge-2/3/1 {
            evc evc1 {
               vlan-list 0-4095;
            }
            evc-map-type all-to-one-bundling;
            uni-id uni-ce2;
         }
      }
   }
}
```

RELATED DOCUMENTATION

connectivity-fault-management

Configuring a CFM Action Profile to Specify CFM Actions for CFM Events

You can create a connectivity fault management (CFM) action profile to define event flags and thresholds to be monitored. You can also specify the action to be taken when any of the configured events occur. When the CFM events occur, the router performs the corresponding action based on your specification. You can configure one or more events in the action profile. Alternatively, you can configure an action profile and specify default actions when connectivity to a remote maintenance association endpoint (MEP) fails.

> **NOTE:** You cannot configure multiple actions at this time. Only one action can be configured. This limitation affects both the **action** and **clear-action** statements.

To configure the CFM action profile:

1. In configuration mode, at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level, specify the name of the action profile and the CFM event(s). You can configure more than one event in the action profile. Possible events include: interface-status-tlv, port-status-tlv, adjacency-loss, RDI.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set action-profile profile-name event [event1, event2, event3..]
   ```

2. Specify the action to be taken by the router when the event occurs. The action is triggered when the event occurs. If you have configured more than one event in the action profile, it is not necessary for all events to occur to trigger the action.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set action-profile profile-name action action
   ```

3. Specify the default action to be taken by the router when connectivity to a remote MEP fails. If no action is configured, no action is taken.

   > **NOTE:** Associating an action profile with the **interface-down** action on an up MEP CFM session running over a circuit cross-connect (CCC) interface (l2circuit/l2vpn) is not advisable and can result in a deadlock situation.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   ```

```
user@host# set action-profile profile-name default-actions action
```

SEE ALSO

event (CFM) | **1793**

default-actions | **1782**

connectivity-fault-management

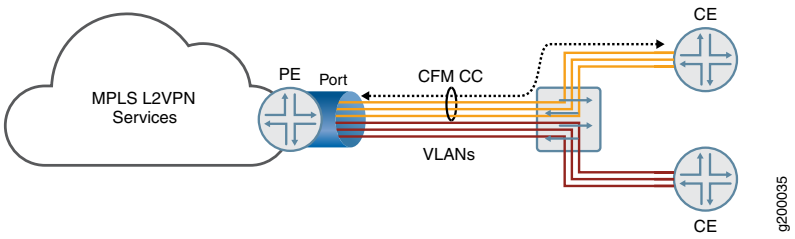
CFM Action Profile to Bring Down a Group of Logical Interfaces Overview

With growing networks, there is a requirement of monitoring a large number of services using CFM. To monitor each service, one session per service logical interface is required. If the services are large in number, this method does not scale as the number of sessions are limited. Instead of one CFM session per service, a single CFM session can monitor multiple services.

Also, there are scenarios where the user-to-network interface (UNI) device needs to be brought down based on sessions on network-to-network Interface (NNI) logical interface. Here, the NNI logical interface refers to core interface and UNI physical interface refers to access interface hosting multiple service logical interfaces. Based on core interface monitoring, you can bring down service logical interfaces associated with access interface.

Figure 5 on page 67 illustrates a topology where a number of services destined to customer-edge (CE) routers share a single port on a provider-edge (PE) router. Each service uses one logical interface. A set of services or logical interfaces (colored in yellow) are destined to one CE router and a set of services or logical interfaces colored in red are destined to another CE router. To monitor each service, you need dedicated down maintenance association end point (MEP) sessions for each service. You can bring down the service by bringing down the service logical interface whenever the session goes down. However, this approach is not scalable if we have large number of services. Monitoring the CFM session on the physical interface is also not feasible because multiple CE routers might be connected and the services to other CE router could be disrupted. To address this issue of monitoring multiple services with a single session, you can create a CCM action profile to bring down a group of logical interfaces by using a CFM session that is configured on a single logical interface.

Figure 5: Topology of Multiple VLAN Services Sharing a Single Port on PE Router Destined to Multiple CE Routers



You can configure CCM action profiles for the following scenarios:

- To bring down a group of logical interfaces all having the same parent port when CCM monitoring session is running on one of the logical interface but on a different parent port.
- To bring down a group of logical interfaces when CCM monitoring session is running on one of the logical interfaces, all belonging to the same parent port.
- To bring down the port, when the CCM monitoring session is running on one of the logical interfaces of a different parent port.

Benefits of Creating CFM Action Profile to Bring Down a Group of Logical Interfaces

- Reduces resource requirement in scaled networks where multiple services need to be monitored.
- Avoids the need to create individual MEP sessions for each service in a topology that includes multiple services to be monitored, thereby enhancing the performance and scalability of the network.

SEE ALSO

action-profile | 1759

Configuring a CFM Action Profile to Bring Down a Group of Logical Interfaces

To monitor multiple services or IFLs using CFM session configured on a single logical interface, you can create a CCM action profile to bring down a group of logical interfaces. You need to define an action to bring down the interface group in the action profile. You will then define the interface device name and the number of logical interfaces that have to be brought down. A logical interface is represented by a combination of the **interface-device-name** and **unit-list**. The following steps explain the procedure to bring down a group of logical interfaces when the **interface-device-name** and/or **unit-list** are specified.

1. In configuration mode, at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level, specify the name of the action profile and the CFM event(s). You can configure more than one event in the action profile.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set action-profile profile-name event [event1, event2, event3..]
```

For example,

```
user@host# set action-profile AP_test event adjacency-loss rdi
```

NOTE: The action **interface-group-down** will not be supported with events other than adjacency-loss and RDI. Any other events configured results in a commit error.

2. In configuration mode, at the [**edit protocols oam ethernet connectivity-fault-management action-profile *profile-name***] hierarchy level, define the action to bring down the interface group.

```
[edit protocols oam ethernet connectivity-fault-management action-profile AP-test ]
user@host# set action interface-group-down
```

NOTE: The action **interface-group-down** will not be supported with other interface related actions. Any other actions configured results in a commit error.

3. At the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level, define the maintenance domain. Specify the maintenance-association parameters.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain domain-name  level number maintenance-association ma-name
   continuity-check interval 1s
```

For example,

```
user@host# set maintenance-domain md6 level 6 maintenance-association ma6 continuity-check interval 1s
```

4. At the **edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name***, define the maintenance association endpoint and the associated parameters.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name]
user@host# set mep mep-id interface interface-name direction down remote -mep mep-id
```

For example,

```
user@host# set mep 101 interface ge-0/0/0.0 direction down remote -mep 102
```

5. If the action-profile has **interface-group-down** action configured, it is mandatory to configure the **interface-group** at the RMEP level. In the configuration mode at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* mep *mep-id* remote-mep *mep-id* action-profile *profile-name*** include the **interface-group** statement to bring down the interface group marked with the action profile as **interface-group-down**.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id remote-mep mep-id action-profile profile-name]
user@host# set interface-group
```

For example,

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md6
   maintenance-association ma6 mep 101 remote-mep 102 action-profile AP_test]
user@host# set interface-group
```

> **NOTE:** If the **interface-group** configuration is not included in the RMEP configuration. The configuration results in commit error.

6. A logical interface is represented by a combination of the **interface-device-name** and **unit-list**. Configure the device interface name and the number of logical interfaces at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* mep *mep-id* remote-mep *mep-id* action-profile *profile-name* interface-group**.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id remote-mep mep-id action-profile profile-name
   interface-group]
user@host# set interface interface-name
user@host# set unit-list logical-interface-unit-number
```

For example,

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md6
  maintenance-association ma6 mep 101 remote-mep 102 action-profile AP_test interface-group]
user@host# set interface ge-0/0/0.0
user@host# set unit-list 1223-3344
```

In this configuration example, the interface ge-0/0/0.0 is brought down.

NOTE:

- At least one of the **interface-group** parameters, **interface-device-name** or **unit-list** must be configured. If the interface device name is not configured, the MEP interface is considered as the device name and the logical interface on that device is brought down.
- If the **unit-list** parameter exceeds the recommended limit, a commit error occurs.
- If the *interface-device-name* is not specified in the **interface-group**, the logical interface numbers mentioned in **unit-list** for the physical interface is brought down.
- If the *unit-list* is not specified in the **interface-group**, IFLs are brought down for the configured interface.

7. Verify the configuration using **show protocols oam** command.

```
[edit]
user@host# show protocols oam
ethernet {
    connectivity-fault-management {
        action-profile AP_TEST {
            event {
                adjacency-loss;
                rdi;
            }
            action {
                interface-group-down;
            }
        }
        maintenance-domain md6 {
            level 6;
            maintenance-association ma6 {
                continuity-check {
                    interval 1s;
                }
                mep 102 {
                    interface ge-0/0/0.0;
```

```
                    direction down;
                    remote-mep 103 {
                        action-profile AP_TEST;
                        interface-group {
                          ge-0/0/1;
                           unit-list [12 23-33 44];
                        }
                    }
                }
            }
        }
    }
}
```

SEE ALSO

interface-group

interface-group-down

Enabling Enhanced Connectivity Fault Management Mode

You can enable enhanced connectivity fault management (CFM) mode to enable effective Ethernet OAM deployment in scaling networks. On enabling enhanced CFM mode, Junos OS supports 32, 000 maintenance association end points (MEPs) and maintenance intermediate points (MIPs) each per chassis for bridge, VPLS, L2VPN, and CCC domains. In previous releases, Junos OS supports 8, 000 MEPs and 8000 MIPS per chassis. If you do not enable enhanced CFM, Junos OS continues to support existing number of MIPs and MEPs per chassis.

NOTE: To support enhanced CFM mode, configure the network services mode on the router as **enhanced-ip**. If the network services mode is not **enhanced-ip**, and you have enabled enhanced CFM, the following warning message is displayed:
[edit protocols oam ethernet]
'connectivity-fault-management'
enhanced ip is not effective please configure enhanced ip and give router reboot

To enable enhanced CFM mode, perform the following steps:

1. In configuration mode, go to the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
```

2. Enable effective Ethernet OAM deployment by enabling enhanced CFM mode.

```
[edit protocols oam ethernet connectivity-fault-management ]
user@host# set enhanced-cfm-mode
```

3. Commit the mode change. A warning message is displayed asking you to restart CFM. If you do not restart CFM, CFM is automatically restarted by Junos OS.

```
[edit protocols oam ethernet connectivity-fault-management ]
user@host # commit
[edit protocols oam ethernet]
'connectivity fault management'
CFM mode change is catastrophic. cfmd will be restarted
commit complete
```

4. To verify if the enhanced CFM mode has been configured, use the **show oam ethernet connectivity-fault-management state** command.

```
[edit protocols oam ethernet connectivity-fault-management ]
user@host# run show oam ethernet connectivity-fault-management
enhanced-cfm-mode;
traceoptions {
    file cfmd.log size 1g;
}
maintenance-domain md6 {
    level 6;
    maintenance-association ma6 {
        continuity-check {
            interval 1s;
        }
        mep 102 {
            interface ge-0/0/0.0;
            direction up;
        }
    }
}
```

SEE ALSO

enhanced-cfm-mode | 1789

Configuring M120 and MX Series Routers for CCC Encapsulated Packets

IN THIS SECTION

- IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview | 73
- CFM Features Supported on Layer 2 VPN Circuits | 73
- Configuring CFM for CCC Encapsulated Packets | 74

IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview

Layer 2 virtual private network (L2VPN) is a type of virtual private network service used to transport customer's private Layer 2 traffic (for example, Ethernet, ATM or Frame Relay) over the service provider's shared IP/MPLS infrastructure. The service provider edge (PE) router must have an interface with circuit cross-connect (CCC) encapsulation to switch the customer edge (CE) traffic to the public network.

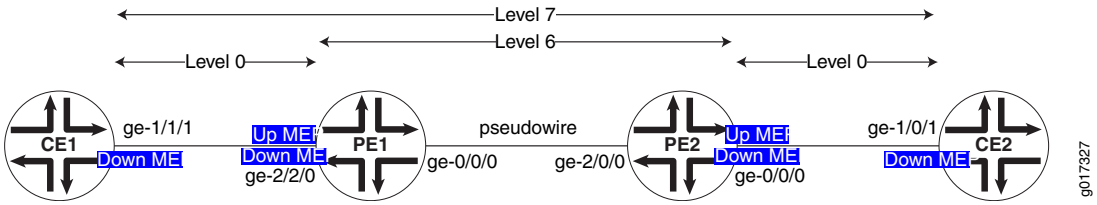
The IEEE 802.1ag Ethernet Connectivity Fault Management (CFM) is an OAM standard used to perform fault detection, isolation, and verification on virtual bridge LANs. M120 and MX Series routers provide CFM support for bridge/VPLS/routed interfaces and support 802.1ag Ethernet OAM for CCC encapsulated packets.

CFM Features Supported on Layer 2 VPN Circuits

CFM features supported on L2VPN circuits are as follows:

- Creation of up/down MEPs at any level on the CE-facing logical interfaces.
- Creation of MIPs at any level on the CE-facing logical interfaces.
- Support for continuity check, loopback, and linkrace protocol.
- Support for the Y1731 Ethernet Delay measurement protocol.
- Support for action profiles to bring the CE-facing logical interfaces down when loss of connectivity is detected.

Figure 6: Layer 2 VPN Topology



To monitor the L2VPN circuit, a CFM up MEP (Level 6 in Figure 6 on page 74) can be configured on the CE-facing logical interfaces of provider edge routers PE1 and PE2. To monitor the CE-PE attachment circuit, a CFM down MEP can be configured on the customer logical interfaces of CE1-PE1 and CE2-PE2 (Level 0 in Figure 6 on page 74).

Configuring CFM for CCC Encapsulated Packets

The only change from the existing CLI configuration is the introduction of a new command to create a MIP on the CE-facing interface of the PE router.

```
protocols {
   oam {
      ethernet {
         connectivity-fault-management {
            # Define a maintenance domains for each default level.
            #; These names are specified as DEFAULT_level_number
            maintenance-domain DEFAULT_x {
               # L2VPN CE interface
               interface (ge | xe)-fpc/pic/port.domain;
            }
            {
            level number;
            maintenance-association identifier {
               mep mep-id {
                  direction (up | down);
                  # L2 VPN CE interface on which encapsulation family CCC is configured.
                  interface (ge | xe)-fpc/pic/port.domain;
                  auto-discovery;
                  priority number;
               }
            }
         }
      }
   }
   }
}
```

SEE ALSO

connectivity-fault-management

Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades

Starting in Release 17.1, Junos OS connectivity fault management (CFM), during a unified in-service software upgrade (ISSU), 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 continuity check message (CCM) PDUs during the unified ISSU. Connectivity fault management continues to operate.

This feature requires the following conditions be met:

- Packet Forwarding Engine keepalives must be enabled to provide inline transmission of CCMs. The feature does not work when the CCMs are transmitted by the CPU of a line card, which is the default transmission method.
- The interval between CCMs must be 1 second.

CFM interoperability during a unified ISSU is supported on the following MPCs: MPC1, MPC2, MPC2-NG, MPC3-NG, MPC5, and MPC6.

To enable CFM interoperability with third-party devices across a unified ISSU:

1. Enable inline keepalives.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

2. Set the CCM interval to 1 second.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name continuity-check]
user@host# set interval 1s
```

SEE ALSO

Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling | 301

Configuring Unified ISSU for 802.1ag CFM

A unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified ISSU is automatically enabled for the Connectivity Fault Management (CFM) protocols and interoperates between local and remote maintenance endpoints (MEPs).

The Junos OS provides support for unified ISSU using the loss threshold type length value (TLV), which is automatically enabled for CFM. TLVs are described in the IEEE 802.1ag standard for CFM as a method of encoding variable-length and optional information in a protocol data unit (PDU). The loss threshold TLV indicates the loss threshold value of a remote MEP. The loss threshold TLV is transmitted as part of the CFM continuity check messages.

> **NOTE:** Starting in Junos OS Release 15.1, configuring ISSU with CFM (802.1ag) is supported only on MX and PTX routers that support TLV. Interoperation with other vendors is not supported.

During a unified ISSU, the control plane may go down for several seconds and cause CFM continuity check packets to get dropped. This may cause the remote MEP to detect a connectivity loss and mark the MEP as down. To keep the MEP active during a unified ISSU, the loss threshold TLV communicates the minimum threshold value the receiving MEP requires to keep the MEP active. The receiving MEP parses the TLV and updates the loss threshold value, but only if the new threshold value is greater than the locally configured threshold value.

An overview of CFM is described starting in "IEEE 802.1ag OAM Connectivity Fault Management Overview" on page 24, and you should further observe the additional requirements described in this topic.

Table 8 on page 76 shows the Loss Threshold TLV format.

Table 8: Loss Threshold TLV Format

Parameter	Octet (sequence)	Description
Type=31	1	Required. Required. If 0, no Length or Value fields follow. If not 0, at least the Length field follows the Type field.
Length=12	2	Required if the Type field is not 0. Not present if the Type field is 0. The 16 bits of the Length field indicate the size, in octets, of the Value field. 0 in the Length field indicates that there is no Value field.
OUI	3	Optional. Organization unique identifier (OUI), which is controlled by the IEEE and is typically the first three bytes of a MAC address (Juniper OUI 0x009069).
Subtype	1	Optional. Organizationally defined subtype.

Table 8: Loss Threshold TLV Format *(continued)*

Parameter	Octet (sequence)	Description
Value	4	Optional. Loss threshold value.
Flag	4	Optional. Bit0 (identifies an ISSU is in progress) Bit1-31 (reserved)

Junos OS provides configuration support for the **convey-loss-threshold** statement, allowing you to control the transmission of the loss threshold TLV in continuity check messages PDUs. The **convey-loss-threshold** statement specifies that the loss threshold TLV must be transmitted as part of the continuity check messages. If the **convey-loss-threshold** statement is not specified, continuity check messages transmit this TLV only when a unified ISSU is in progress. The Junos OS provides this configuration at the continuity-check level. By default, continuity check messages do not include the loss threshold TLV.

To configure the convey loss threshold, use the **convey-loss-threshold** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *identifier* maintenance-association *identifier* continuity-check]** hierarchy level.

For the remote MEP, the loss threshold TLV is transmitted only during the unified ISSU if the **convey-loss-threshold** statement is not configured. The remote MEP switches back to the default loss threshold if no loss threshold TLV is received or the TLV has a default threshold value of 3.

An example of the ISSU configuration statements follows:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                level number;
                    maintenance-association identifier {
                        continuity-check {
                            convey-loss-threshold;
                            interval number;
                            loss-threshold number;
                            hold-interval number;
                        }
                    }
                }
            }
        }
    }
```

```
  }
```

The Junos OS saves the last received loss threshold TLV from the remote MEP. You can display the last saved loss threshold TLV that is received by the remote MEP, using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md3* maintenance-association *ma5* local-mep *2* remote-mep *1***

```
Maintenance domain name: md3, Format: string, Level: 3
  Maintenance association name: ma3, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 2, Direction: up, MAC address: 00:19:e2:b0:76:be
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: yes
    Prefer me: no, Protection in use: no, FRR Flag: no
  Interface name: xe-4/1/1.0, Interface status: Active, Link status: Up
    Loss Threshold TLV:
      Loss Threshold: 3  , Flag:    0x0

 Remote MEP identifier: 1, State: ok
    MAC address: 00:1f:12:b7:ce:79, Type: Learned
    Interface: xe-4/1/1.0
    Last flapped: Never
    Continuity: 100%, Admin-enable duration: 45sec, Oper-down duration: 0sec
    Effective loss threshold: 3 frames
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
    Connection Protection TLV:
      Prefer me: no, Protection in use: no, FRR Flag: no
    Loss Threshold TLV:   #Displays last received value
      Loss Threshold: 3  , Flag:    0x0
```

The Junos OS saves the last transmitted loss threshold TLV from a local MEP. You can display the last transmitted loss threshold TLV and the effective loss (operational) threshold for the remote MEP, using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier***

maintenance-association *identifier* local-mep *identifier* remote-mep *identifier* command, as in the following example:

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md3 maintenance-association ma5 local-mep 2 remote-mep 1
```

```
Maintenance domain name: md3, Format: string, Level: 3
  Maintenance association name: ma3, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 2, Direction: up, MAC address: 00:19:e2:b0:76:be
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: yes
    Prefer me: no, Protection in use: no, FRR Flag: no
  Interface name: xe-4/1/1.0, Interface status: Active, Link status: Up
    Loss Threshold TLV:   #Displays last transmitted value
      Loss Threshold: 3  , Flag:    0x0

   Remote MEP identifier: 1, State: ok
    MAC address: 00:1f:12:b7:ce:79, Type: Learned
    Interface: xe-4/1/1.0
    Last flapped: Never
    Continuity: 100%, Admin-enable duration: 45sec, Oper-down duration: 0sec
    Effective loss threshold: 3 frames   #Displays operational threshold
    Remote defect indication: falsePort status TLV: none
    Interface status TLV: none
    Connection Protection TLV:
      Prefer me: no, Protection in use: no, FRR Flag: no
    Loss Threshold TLV:
      Loss Threshold: 3  , Flag:    0x0
```

SEE ALSO

> *Before You Begin a Unified ISSU*
>
> *Unified ISSU System Requirements*

Junos OS Support for Performance Monitoring Compliant with Technical Specification MEF 36

Junos OS release 16.1R1 and later supports performance monitoring that is compliant with Technical Specification MEF 36. Technical Specification MEF 36 specifies the performance monitoring MIB. The performance monitoring MIB is required to manage service operations, administration, and maintenance

(OAM) implementations that satisfy the Service OAM requirements and framework specified in MEF 17 and MEF 35, the management objects specified in MEF 7.1, and the performance monitoring functions defined in ITU-T Y.1731 and IEEE 802.1ag.

You can enable MEF-36-compliant performance monitoring by configuring the **measurement-interval** statement at the **[edit protocols oam ethernet cfm performance-monitoring]** hierarchy level.

When MEF-36-compliant performance monitoring is enabled:

- An SNMP get next request for a variable might not fetch the current value unless an SNMP walk is performed before performing the get next request. This limitation applies only to the current statistics for delay measurement, loss measurement, and synthetic loss measurement.
- The output for the field **Current delay measurement statistics** might display a measurement interval of 0 (zero) and an incorrect timestamp until the first cycle time has expired.
- Supported data TLV size for performance monitoring protocol data units (PDUs) is 1386 bytes when MEF-36-compliant performance monitoring is enabled. The TLV size is 1400 bytes in legacy mode.
- The maximum configurable value for the lower threshold bin is 4,294,967,294.
- Frame loss ratio (FLR) is excluded in loss measurements during period of unavailability for synthetic loss measurement only. In case of loss measurement, FLR is included even during period of unavailability.
- During a period of loss of continuity (adjacency down), although SOAM PDUs are not sent, FLR and availability calculations are not stopped. These calculations are performed with the assumption of 100% loss.
- The number of SOAM PDUs that are sent during the first measurement interval might be less than expected. This is because of a delay in detecting the adjacency state at the performance monitoring session level.
- The number of SOAM PDUs transmitted during a measurement interval for a cycle time of 100 ms might not be accurate. For example, in a measurement interval of two minutes with a cycle time 100 ms, the SOAM PDUs transmitted might be in the range of 1198—2000.

SEE ALSO

measurement-interval | **1821**

Damping CFM performance Monitoring Traps and Notifications to Prevent Congestion of The NMS

You can dampen the performance monitoring threshold-crossing traps and notifications that are generated every time a threshold-crossing event occurs to prevent congestion of the network management system (NMS).

Damping limits the number of jnxSoamPmThresholdCrossingAlarm traps sent to the NMS by summarizing the flap occurrences over a period of time, known as the flap trap timer, and sends a single jnxSoamPmThresholdFlapAlarm notification to the NMS. You can configure the duration of the flap trap timer to any value from 1 through 360 seconds.

The jnxSoamPmThresholdFlapAlarm notification is generated and sent when the following conditions are met:

- At least one flap has occurred when the flap timer has expired.
- You changed the value of the flap trap timer, which caused the timer to stop.

You can enable damping at the global level for the iterator or you can enable damping at the individual threshold type of the iterator. For instance, to enable damping at the global level, for the iterator, use the following command: **set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles *profile-name* flap-trap-monitor**. To enable damping at a specific threshold type, for the **avg-fd-twoway-threshold**, use the following command: **set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles *profile-name* avg-fdv-twoway-threshold flap-trap-monitor**.

You can also disable damping.

SEE ALSO

flap-trap-monitor | 1794

Physical Interface Damping Overview

Example: Configuring Ethernet CFM on Physical Interfaces

IN THIS SECTION

- Requirements | 82
- Overview | 82
- Configuration | 82

This example shows the configuration of Ethernet connectivity fault management (CFM) on physical interfaces.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.3 or later.

Overview

CFM can be used to monitor the physical link between two routers. This functionality is similar to that supported by the IEEE 802.3ah LFM protocol.

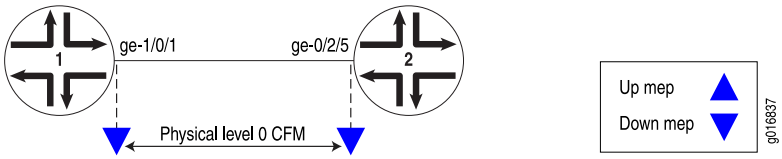
In Junos OS Release 9.3 and later, CFM also supports aggregated Ethernet interfaces. On interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers, CFM is not supported on untagged aggregated Ethernet member links. MPCs and MICs do support CFM on untagged and tagged aggregated Ethernet logical interfaces.

> **NOTE:** The configurations in this example are only partial examples of complete and functional router configurations. Do not copy these configurations and use them directly on an actual system.

Configuration

In the following example, two routers (Router 1 and Router 2) are connected by a point-to-point Gigabit Ethernet link. The link between these two routers is monitored using CFM. This is shown in Figure 7 on page 82. The single boundary is a “down mep” in CFM terminology.

Figure 7: Ethernet CFM on Physical Interfaces



To configure Ethernet CFM on physical interfaces, perform these tasks:

CLI Quick Configuration
Router 1

Configure the interface and CFM:

```
[edit]
interfaces ge-1/0/1 {
    unit 0 {
        family inet;
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 100 {
                            interface ge-1/0/1;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

The configuration on Router 2 mirrors that on Router 1, with the exception of the *mep-id*.

Router 2

Configure the interface and CFM:

```
[edit]
interfaces ge-0/2/5 {
    unit 0 {
```

```
        family inet;
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 200 {
                            interface ge-0/2/5;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

To verify that the physical interface is configured correctly for CFM, use the **show interface** command. To verify the CFM configuration, use one or more of the **show oam ethernet connectivity-fault-management** commands listed in the CLI Explorer.

SEE ALSO

show oam ethernet connectivity-fault-management interfaces | 2727

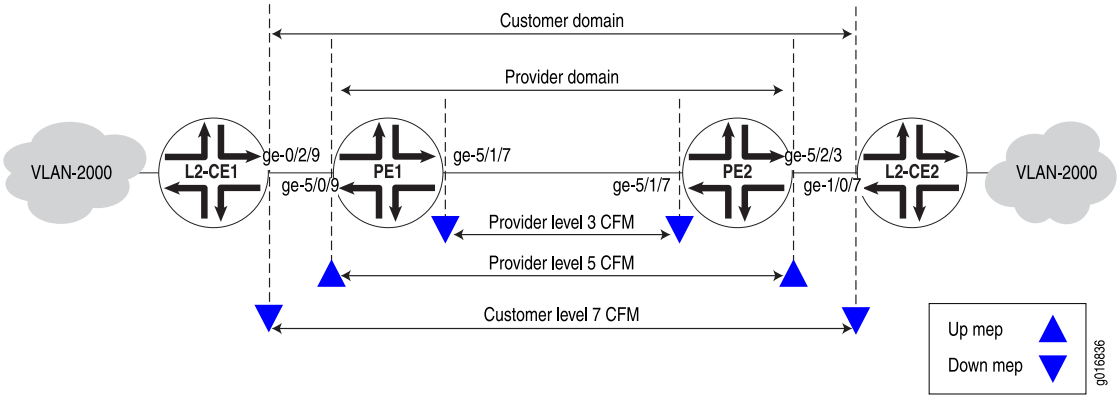
Example: Configuring Ethernet CFM on Bridge Connections

In this example, both the customer and service provider are running Ethernet CFM over a simple bridge network. The network is shown in Figure 8 on page 85. The customer has configured Ethernet CFM on MX Series routers L2-CE1 and L2-CE2. The service provider has configured Ethernet CFM on MX Series routers PE1 and PE2.

NOTE: The configurations in this example are only partial examples of complete and functional router configurations. Do not copy these configurations and use them directly on an actual system.

The service provider is using CFM level 3 for the link between PE1 and PE2 and level 5 from one CE facing port to the other. The customer is using CFM level 7. The boundaries are marked with “up mep” and “down mep” CFM terminology in the figure.

Figure 8: Ethernet CFM over a Bridge Network



Here are the configurations of CFM on the customer routers.

CFM on L2-CE1

```
[edit interfaces]
ge-0/2/9 {
   vlan-tagging;
   unit 0 {
      vlan-id 2000;
   }
}

[edit protocols oam ethernet]
connectivity-fault-management {
   maintenance-domain customer {
      level 7;
      maintenance-association customer-site1 {
         continuity-check {
            interval 1s;
```

```
            }
            mep 700 {
                interface ge-0/2/9.0;
                direction down;
                auto-discovery;
            }
        }
    }
}
```

CFM on L2-CE2

```
[edit interfaces]
ge-1/0/7 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam ethernet]
connectivity-fault-management {
    maintenance-domain customer {
        level 7;
        maintenance-association customer-site2 {
            continuity-check {
                interval 1s;
            }
            mep 800 {
                interface ge-1/0/7.0;
                direction down;
                auto-discovery;
            }
        }
    }
}
```

Here are the configurations of CFM on the provider routers.

CFM on PE1

```
[edit interfaces]
ge-5/0/9 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}
ge-5/1/7 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}

[edit bridge-domains]
bridge-vlan2000 {
    domain-type bridge;
    vlan-id 2000;
    interface ge-5/0/9.0;
    interface ge-5/1/7.0;
}

[edit protocols oam ethernet connectivity-fault-management]
maintenance-domain provider-outer {
    level 5;
    maintenance-association provider-outer-site1 {
        continuity-check {
            interval 1s;
        }
        mep 200 {
            interface ge-5/0/9.0;
            direction up;
            auto-discovery;
        }
    }
}
maintenance-domain provider-inner {
    level 3;
```

```
    maintenance-association provider-inner-site1 {
        continuity-check {
            interval 1s;
        }
        mep 200 {
            interface ge-5/1/7.0;
            direction down;
            auto-discovery;
        }
    }
}
```

CFM on PE2

```
[edit interfaces]
ge-5/1/7 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}
ge-5/2/3 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}

[edit bridge-domains]
bridge-vlan2000 {
    domain-type bridge;
    interface ge-5/2/3.0;
    interface ge-5/1/7.0;
}

[edit protocols oam ethernet connectivity-fault-management]
```

```
maintenance-domain provider-outer {
    level 5;
    maintenance-association provider-outer-site1 {
        continuity-check {
            interval 1s;
        }
        mep 100 {
            interface ge-5/2/3.0;
            direction up;
            auto-discovery;
        }
    }
}
maintenance-domain provider-inner {
    level 3;
    maintenance-association provider-inner-site1 {
        continuity-check {
            interval 1s;
        }
        mep 100 {
            interface ge-5/1/7.0;
            direction down;
            auto-discovery;
        }
    }
}
```

SEE ALSO

Configuring Continuity Check Messages | 124

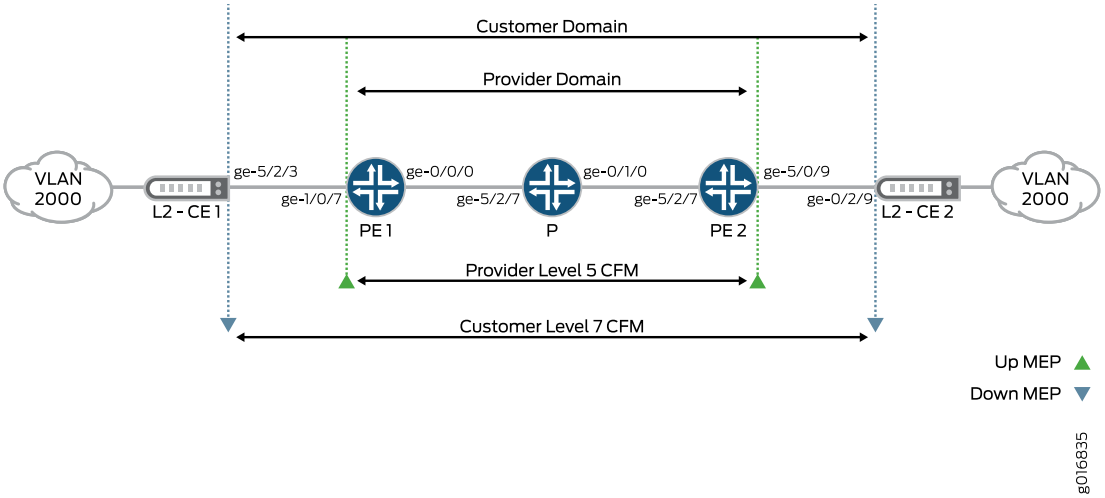
Example: Configuring Ethernet CFM over VPLS

In this example, both the customer and service provider are running Ethernet CFM over a VPLS and a multiprotocol label switching (MPLS) network. The network is shown in Figure 9 on page 90. The customer has configured Ethernet CFM on MX Series routers L2-CE1 and L2-CE2. The service provider has configured Ethernet CFM on MX Series routers PE1, P, and PE2.

NOTE: The configurations in this example are only partial examples of complete and functional router configurations. Do not copy these configurations and use them directly on an actual system.

The service provider is using CFM level 5 and the customer is using CFM level 7. The boundaries are marked with “up mep” and “down mep” CFM terminology in the figure.

Figure 9: Ethernet OAM with VPLS



NOTE: The logical interfaces in a VPLS routing instance might have the same or different VLAN configurations. VLAN normalization is required to switch packets correctly among these interfaces. Normalization supports automatic mapping of VLANs and performs operations on VLAN tags to achieve the desired translation. See *Configuring a Normalized VLAN for Translation or Tagging*.

NOTE:

The following forwarding path considerations must be observed:

- Packet receive path:
  - This is the forwarding path for packets received on the interfaces.
  - 802.1ag Ethernet OAM for VPLS uses implicit interface filters and forwarding table filters to flood, accept, and drop the CFM packets.
- Packet transmit path:
  - Junos OS uses the router's hardware-based forwarding for CPU-generated packets.
  - For down MEPs, the packets are transmitted on the interface on which the MEP is configured.
  - In MX series routers, for up MEPs, the packets must be flooded to other interfaces in the VPLS routing instance. The router creates a flood route tied to a flood next hop (with all interfaces to flood) and then sources the packets to be forwarded with this flood route.

The following are the configurations of the VPLS and CFM on the service provider routers.

Configuration of PE1

```
[edit chassis]
fpc 5 {
    pic 0 {
        tunnel-services {
            bandwidth 1g;
        }
    }
}

[edit interfaces]
ge-1/0/7 {
    encapsulation flexible-ethernet-services;
    vlan-tagging;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 2000;
    }
}
ge-0/0/0 {
```

```
    unit 0 {
        family inet {
            address 10.200.1.1/24;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.168.231/32 {
                primary;
            }
            address 127.0.0.1/32;
        }
    }
}

[edit routing-instances]
vpls-vlan2000 {
    instance-type vpls;
    vlan-id 2000;
    interface ge-1/0/7.1;
    route-distinguisher 10.255.168.231:2000;
    vrf-target target:1000:1;
    protocols {
        vpls {
            site-range 10;
            site vlan2000-PE1 {
                site-identifier 2;
            }
        }
    }
}

[edit protocols]
rsvp {
    interface ge-0/0/0.0;
}
mpls {
    label-switched-path PE1-to-PE2 {
        to 10.100.1.1;
```

```
    }
    interface ge-0/0/0.0;
}
bgp {
    group PE1-to-PE2 {
        type internal;
        local-address 10.200.1.1;
        family l2vpn {
            signaling;
        }
        local-as 65000;
        neighbor 10.100.1.1;
    }
}
ospf {
    traffic-engineering;
    reference-bandwidth 4g;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
        interface ge-0/0/0.0;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain customer-site1 {
                level 5;
                maintenance-association customer-site1 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 100 {
                        interface ge-1/0/7.1;
                        direction up;
                        auto-discovery;
                    }
                }
            }
        }
```

```
    }
}
```

Configuration of PE2

```
[edit chassis]
fpc 5 {
    pic 0 {
        tunnel-services {
            bandwidth 1g;
        }
    }
}

[edit interfaces]
ge-5/0/9 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 2000;
    }
}
ge-5/2/7 {
    unit 0 {
        family inet {
            address 10.100.1.1/24;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.168.230/32 {
                primary;
            }
            address 127.0.0.1/32;
        }
    }
```

```
}

[edit routing-instances]
vpls-vlan2000 {
    instance-type vpls;
    vlan-id 2000;
    interface ge-5/0/9.1;
    route-distinguisher 10.255.168.230:2000;
    vrf-target target:1000:1;
    protocols {
        vpls {
            site-range 10;
            site vlan2000-PE2 {
                site-identifier 1;
            }
        }
    }
}

[edit protocols]
rsvp {
    interface ge-5/2/7.0;
}
mpls {
    label-switched-path PE2-to-PE1 {
        to 10.200.1.1;
    }
    interface ge-5/2/7.0;
}
bgp {
    group PE2-to-PE1 {
        type internal;
        local-address 10.100.1.1;
        family l2vpn {
            signaling;
        }
        local-as 65000;
        neighbor 10.200.1.1;
    }
}
ospf {
    traffic-engineering;
```

```
    reference-bandwidth 4g;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
        interface ge-5/2/7.0;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain customer-site1 {
                level 5;
                maintenance-association customer-site1 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 200 {
                        interface ge-5/0/9.1;
                        direction up;
                        auto-discovery;
                    }
                }
            }
        }
    }
}
```

Configuration of P router

MPLS only, no CFM needed:

```
[edit]
interfaces {
    ge-5/2/7 {
        # Connected to PE1
        unit 0 {
            family inet {
                address 10.200.1.10/24;
```

```
            }
            family mpls;
        }
    }
    ge-0/1/0 {
        # Connected to PE2
        unit 0 {
            family inet {
                address 10.100.1.10/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0{
            family inet {
                address 10.255.168.240/32;
            }
        }
    }
}

[edit]
protocols {
    rsvp {
        interface ge-0/1/0.0;
        interface ge-5/2/7.0;
    }
    mpls {
        interface ge-0/1/0.0;
        interface ge-5/2/7.0;
    }
    ospf {
        traffic-engineering;
        reference-bandwidth 4g;
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
            interface ge-0/1/0.0;
            interface ge-5/2/7.0;
```

```
        }
    }
}
```

CFM on L2-CE1

Here is the configuration of CFM on L2-E1:

```
[edit interfaces]
ge-5/2/3 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam]
ethernet {
    connectivity-fault-management {
        maintenance-domain customer {
            level 7;
            maintenance-association customer-site1 {
                continuity-check {
                    interval 1s;
                }
                mep 800 {
                    interface ge-5/2/3.0;
                    direction down;
                    auto-discovery;
                }
            }
        }
    }
}
```

CFM on L2-CE2

Here is the configuration of CFM L2-CE2:

```
[edit interfaces]
ge-0/2/9 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam]
ethernet {
    connectivity-fault-management {
        maintenance-domain customer {
            level 7;
            maintenance-association customer-site1 {
                continuity-check {
                    interval 1s;
                }
                mep 700 {
                    interface ge-0/2/9.0;
                    direction down;
                    auto-discovery;
                }
            }
        }
    }
}
```

SEE ALSO

Configuring Continuity Check Messages | 124

Release History Table

Release	Description
17.1	Starting in Release 17.1, Junos OS connectivity fault management (CFM), during a unified in-service software upgrade (ISSU), works when the peer device is not a Juniper Networks router.
15.1	Starting in Junos OS Release 15.1, configuring ISSU with CFM (802.1ag) is supported only on MX and PTX routers that support TLV.
12.3	Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs.
12.3	Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs.
12.3	Starting with Junos OS Release 12.3, for all interfaces configured on Modular Port Concentrators (MPCs) on MX Series 5G Universal Routing Platforms, you no longer need to configure the **no-control-word** statement for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs.

RELATED DOCUMENTATION

Configuring Continuity Check Messages | **124**

Inline Transmission Mode | **300**

CFM Monitoring between CE and PE Devices

IN THIS SECTION

- Understanding CFM Monitoring between CE and PE Devices | **101**
- Configuring Port Status TLV and Interface Status TLV | **102**
- Configuring Chassis ID TLV | **116**

Configuring MAC Flush Message Processing in CET Mode | 118
Example: Configuring an Action Profile Based on Connection Protection TLVs | 121

Use this topic to understand more about CFM monitoring between provider edge devices and customer edge devices when the customer edge device is not a Juniper device. Also, you can understand more about how Interface Status TLVs, port status TLVs, chassis ID TLV, and connection protection TLV help in monitoring your network.

Understanding CFM Monitoring between CE and PE Devices

You can enable connectivity fault management (CFM) monitoring between provider edge devices and customer edge devices when the customer edge device is not a Juniper device. When the interface is down, CFM propagates the status of the interface in the CC messages. The CC message informs the customer edge device that the provider edge device is down.

You can configure CFM monitoring using either of the following two options:

- Interface Status TLV (Type, Length, and Value)—You can enable connectivity fault management (CFM) monitoring between provider edge devices and customer edge devices when the customer edge device is not a Juniper device by using Interface Status TLV. When the interface is down, CFM propagates the status of the interface using interface status TLV. The Interface Status TLV indicates the status of the interface on which the MEP transmitting the CCM is configured, or the next-lower interface in the IETF RFC 2863 IF-MIB. Thus, the customer edge device is aware that the provider edge device is down. To configure CFM monitoring using Interface Status TLV, use the **interface-status-tlv** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain*maintenance-association *maintenance-association* continuity-check** hierarchy level. This is the standard option.
- RDI (Remote Defect Indication)—Starting in Junos OS Release 17.3R1, you can enable connectivity fault management (CFM) monitoring between provider edge devices and customer edge devices when the customer edge device is not a Juniper device by using the remote defect indication (RDI) bit. When you enable CFM monitoring, CFM propagates the status of the provider edge device via the remote defect indication (RDI) bit in the CC messages. Thus, the customer edge device is aware that the provider edge device is down. The RDI bit is cleared when the service is back up. To configure CFM monitoring using the RDI bit, use the **interface-status-send-rdi** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain*maintenance-association *maintenance-association* continuity-check** hierarchy level. This option is required if the customer edge device does not support Interface Status TLV.

NOTE: When the interface is set to CCC down and you have configured RDI, then RDI bit is sent. CFM does not monitor the status of the interface. If CCC down is set when the interface is not standby, RDI bit is sent with the CC messages if you have configured RDI.

Single Active Multi-homing Use Case using RDI bit

Consider the following topology where there are two provider edge devices (PE1 and PE2) as well as two customer edge devices (CE1 and CE2). PE1 is in active state while PE2 is in standby state. CFM down MEP is configured between the PE and CE. CFM detects that the CCC down and because CFM down MEP is configured, the CC messages generated have the RDI bit. The CC messages from PE2 to CE2 have the RDI bit set to indicate the blocked state. When PE2 becomes active, CCM down is cleared and the RDI bit is cleared from the subsequent CC messages.

Active/Active Multihoming Use case using RDI bit

Consider the topology where there are two provider edge devices (PE1 and PE2) and two customer edge devices (CE1 and CE2). PE1 is in active state while PE2 is in standby state. If CFM down MEP is not configured between the PE and CE to monitor the link connectivity, the CC messages generated do not have the RDI bit. CFM down MEP is configured between the PE and CE. CFM detects that the CCC down and because CFM down MEP is configured, the CC messages generated have the RDI bit. The CC messages from PE2 to CE2 have the RDI bit set to indicate the blocked state. When PE2 becomes active, CCM down is cleared and the RDI bit is cleared from the subsequent CC messages.

SEE ALSO

interface-status-tlv | **1804**

interface-status-send-rdi | **1805**

Configuring Port Status TLV and Interface Status TLV

IN THIS SECTION

- TLVs Overview | **103**
- Various TLVs for CFM PDUs | **103**
- Support for Additional Optional TLVs | **105**
- MAC Status Defects | **112**
- Configuring Remote MEP Action Profile Support | **114**
- Monitoring a Remote MEP Action Profile | **115**

TLVs Overview

Type, Length, and Value (TLVs) are described in the IEEE 802.1ag standard for CFM as a method of encoding variable-length and/or optional information in a PDU. TLVs are not aligned to any particular word or octet boundary. TLVs follow each other with no padding between them.

Table 9 on page 103 shows the TLV format and indicates if it is required or optional.

Table 9: Format of TLVs

Parameter	Octet (sequence)	Description
Type	1	Required. If 0, no Length or Value fields follow. If not 0, at least the Length field follows the Type field.
Length	2–3	Required if the Type field is not 0. Not present if the Type field is 0. The 16 bits of the Length field indicate the size, in octets, of the Value field. 0 in the Length field indicates that there is no Value field.
Value	4	Length specified by the Length field. Optional. Not present if the Type field is 0 or if the Length field is 0.

Various TLVs for CFM PDUs

Table 10 on page 103 shows a set of TLVs defined by IEEE 802.1ag for various CFM PDU types. Each TLV can be identified by the unique value assigned to its type field. Some type field values are reserved.

Table 10: Type Field Values for Various TLVs for CFM PDUs

TLV or Organization	Type Field
End TLV	0
Sender ID TLV	1
Port Status TLV	2
Data TLV	3
Interface Status TLV	4
Reply Ingress TLV	5
Reply Egress TLV	6
LTM Egress Identifier TLV	7
LTR Egress Identifier TLV	8

Table 10: Type Field Values for Various TLVs for CFM PDUs *(continued)*

TLV or Organization	Type Field
Reserved for IEEE 802.1	9 to 30
Organization-Specific TLV	31
Defined by ITU-T Y.1731	32 to 63
Reserved for IEEE 802.1	64 to 255

Not every TLV is applicable for all types of CFM PDUs.

- TLVs applicable for continuity check message (CCM):
  - End TLV
  - Sender ID TLV
  - Port Status TLV
  - Interface Status TLV
  - Organization-Specific TLV
- TLVs applicable for loopback message (LBM):
  - End TLV
  - Sender ID TLV
  - Data TLV
  - Organization-Specific TLV
- TLVs applicable for loopback reply (LBR):
  - End TLV
  - Sender ID TLV
  - Data TLV
  - Organization-Specific TLV
- TLVs applicable for linktrace message (LTM):
  - End TLV
  - LTM Egress Identifier TLV

  - Sender ID TLV
  - Organization-Specific TLV
- TLVs applicable for linktrace reply (LTR):
  - End TLV
  - LTR Egress Identifier TLV
  - Reply Ingress TLV
  - Reply Egress TLV
  - Sender ID TLV
  - Organization-Specific TLV

The following TLVs are currently supported in the applicable CFM PDUs:

- End TLV
- Reply Ingress TLV
- Reply Egress TLV
- LTR Egress Identifier TLV
- LTM Egress Identifier TLV
- Data TLV

Support for Additional Optional TLVs

IN THIS SECTION

Port Status TLV | **106**
Interface Status TLV | **109**

The following additional optional TLVs are supported:

- Port Status TLV
- Interface Status TLV

MX Series routers support configuration of port status TLV and interface status TLV. Configuring the Port Status TLV allows the operator to control the transmission of the Port Status TLV in CFM PDUs.

NOTE: Although Port Status TLV configuration statements are visible in the CLI on M120 and M320 routers, Port Status TLV cannot be configured on these systems. Port Status TLV can be enabled on a MEP interface only if it is a bridge logical interface, which is not possible on these systems.

For configuration information, see the following sections:

Port Status TLV

The Port Status TLV indicates the ability of the bridge port on which the transmitting MEP resides to pass ordinary data, regardless of the status of the MAC. The value of this TLV is driven by the MEP variable **enableRmepDefect**, as shown in Table 12 on page 106. The format of this TLV is shown in Table 11 on page 106.

Any change in the Port Status TLVs value triggers one extra transmission of that bridge ports MEP CCMs.

Table 11: Port Status TLV Format

Parameter	Octet (Sequence)
Type = 2	1
Length	2–3
Value (See Table 12 on page 106)	4

Table 12: Port Status TLV Values

Mnemonic	Ordinary Data Passing Freely Through the Port	Value
psBlocked	No: **enableRmepDefect** = false	1
psUp	Yes: **enableRmepDefect** = true	2

The MEP variable **enableRmepDefect** is a boolean variable indicating whether frames on the service instance monitored by the maintenance associations if this MEP are enabled to pass through this bridge port by the Spanning Tree Protocol and VLAN topology management. It is set to TRUE if:

- The bridge port is set in a state where the traffic can pass through it.
- The bridge port is running multiple instances of the spanning tree.
- The MEP interface is not associated with a bridging domain.

Configuring Port Status TLV

Junos OS provides configuration support for the Port Status TLV, allowing you to control the transmission of this TLV in CCM PDUs. The Junos OS provides this configuration at the continuity-check level. By default, the CCM does not include the Port Status TLV. To configure the Port Status TLV, use the **port-status-tlv** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *identifier* maintenance-association *identifier* continuity-check]** hierarchy level.

> **NOTE:** Port Status TLV configuration is not mandated by IEEE 802.1ag. The Junos OS provides it in order to give more flexibility to the operator; however it receives and processes CCMs with a Port Status TLV, regardless of this configuration.

An example of the configuration statements follows:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                level number;
                    maintenance-association identifier {
                        continuity-check {
                            interval number,
                            loss-threshold number;
                            hold-interval number;
                            port-status-tlv; # Sets Port Status TLV
                        }
                    }
                }
            }
        }
    }
}
```

You cannot enable Port Status TLV transmission in the following two cases:

- If the MEP interface under the maintenance-association is not of type bridge.
- If the MEP is configured on a physical interface.

Displaying the Received Port Status TLV

The Junos OS saves the last received Port Status TLV from a remote MEP. If the received Port Status value does not correspond to one of the standard values listed in Table 12 on page 106, then the **show** command displays it as "unknown." You can display the last saved received Port Status TLV using the **show oam**

ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier* command, as in the following example:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md5* maintenance-association *ma5* local-mep *2001* remote-mep *1001***

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none # RX PORT STATUS
    Interface status TLV: none
```

Displaying the Transmitted Port Status TLV

The Junos OS saves the last transmitted Port Status TLV from a local MEP. If the transmission of the Port Status TLV has not been enabled, then the **show** command displays "none." You can display the last saved transmitted Port Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md5* maintenance-association *ma5* local-mep *2001* remote-mep *1001***

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up # TX PORT STATUS
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
```

```
MAC address: 00:19:e2:b0:74:00, Type: Learned
Interface: ge-2/0/0.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: none
```

Interface Status TLV

The Interface Status TLV indicates the status of the interface on which the MEP transmitting the CCM is configured, or the next-lower interface in the IETF RFC 2863 IF-MIB. The format of this TLV is shown in Table 13 on page 109. The enumerated values are shown in Table 14 on page 109.

Table 13: Interface Status TLV Format

Parameter	Octet (Sequence)
Type = 4	1
Length	2–3
Value (See Table 14 on page 109)	4

Table 14: Interface Status TLV Values

Mnemonic	Interface Status	Value
isUp	up	1
isDown	down	2
isTesting	testing	3
isUnknown	unknown	4
isDormant	dormant	5
isNotPresent	notPresent	6
isLowerLayerDown	lowerLayerDown	7

NOTE: When the operational status of a logical interface changes from the down state (status value of 2) to the lower layer down state (status value of 7) and vice versa, the LinkDown SNMP trap is not generated. For example, if you configure an aggregated Ethernet interface bundle with a VLAN tag and add a physical interface that is in the operationally down state to the bundle, the operational status of the aggregated Ethernet logical interface bundle at that point is lower layer down (7). If you take the MIC associated with the interface offline, the LinkDown trap is not generated when the logical interface shifts from the lower layer down state to the down state.

Similarly, consider another sample scenario in which an physical interface is added to an aggregated Ethernet bundle that has VLAN tagging and the aggregated Ethernet logical interface is disabled. When the logical interface is disabled, the operational status of the logical interface changes to down. If you disable the physical interface that is part of the aggregated Ethernet bundle, the operational status of the aggregated Ethernet logical interface remains down. If you reenable the aggregated Ethernet logical interface, the operational status of it changes from down to lower layer down. The LinkDown SNMP trap is not generated at this point.

Configuring Interface Status TLV

The Junos OS provides configuration support for the Interface Status TLV, thereby allowing operators to control the transmission of this TLV in CCM PDUs through configuration at the continuity-check level.

NOTE: This configuration is not mandated by IEEE 802.1ag; rather it is provided to give more flexibility to the operator. The Junos OS receives and processes CCMs with the Interface Status TLV, regardless of this configuration.

The interface status TLV configuration is shown below:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                    level number;
                    maintenance-association identifier {
                        continuity-check {
                            interval number;
                            loss-threshold number;
                            hold-interval number;
```

```
                interface-status-tlv; # Sets the interface status TLV
              }
            }
          }
        }
      }
    }
  }
```

NOTE: The Junos OS supports transmission of only three out of seven possible values for the Interface Status TLV. The supported values are 1, 2, and 7. However, the Junos OS is capable of receiving any value for the Interface Status TLV.

Displaying the Received Interface Status TLV

The Junos OS saves the last received Interface Status TLV from the remote MEP. If the received Interface Status value does not correspond to one of the standard values listed in Table 13 on page 109, then the **show** command displays "unknown."

You can display this last saved Interface Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md5* maintenance-association *ma5* local-mep *2001* remote-mep *1001***

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
```

```
    Port status TLV: none
    Interface status TLV: none # displays the Interface Status TLV state
```

Displaying the Transmitted Interface Status TLV

The Junos OS saves the last transmitted Interface Status TLV from a local MEP. If the transmission of Interface Status TLV has not been enabled, then the **show** command displays "none."

You can display the last transmitted Interface Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md5* maintenance-association *ma5* local-mep *2001* remote-mep *1001***

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
```

MAC Status Defects

The Junos OS provides MAC status defect information, indicating that one or more of the remote MEPs is reporting a failure in its Port Status TLV or Interface Status TLV. It indicates “yes” if either some remote MEP is reporting that its interface is not isUp (for example, at least one remote MEPs interface is unavailable), or if all remote MEPs are reporting a Port Status TLV that contains some value other than psUp (for example, all remote MEPs Bridge Ports are not forwarding data). There are two **show** commands you can use to view the MAC Status Defects indication.

Use the **mep-database** command to display MAC status defects:

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md6* maintenance-association *ma6***

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM            : no
    Erroneous CCM received                  : no
    Cross-connect CCM received              : no
    RDI sent by some MEP                    : no
    Some remote MEP's MAC in error state    : yes # MAC Status Defects yes/no
  Statistics:
    CCMs sent                               : 1658
    CCMs received out of sequence           : 0
    LBMs sent                               : 0
    Valid in-order LBRs received            : 0
    Valid out-of-order LBRs received        : 0
    LBRs received with corrupted data       : 0
    LBRs sent                               : 0
    LTMs sent                               : 0
    LTMs received                           : 0
    LTRs sent                               : 0
    LTRs received                           : 0
    Sequence number of next LTM request     : 0
    1DMs sent                               : 0
    Valid 1DMs received                     : 0
    Invalid 1DMs received                   : 0
    DMMs sent                               : 0
    DMRs sent                               : 0
    Valid DMRs received                     : 0
    Invalid DMRs received                   : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      200     00:05:85:73:39:4a       ok    xe-5/0/0.0
```

Use the **interfaces** command to display MAC status defects:

user@host> **show oam ethernet connectivity-fault-management interfaces detail**

```
Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
  Maintenance domain name: md6, Format: string, Level: 6
    Maintenance association name: ma6, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: up, Port status TLV: up
    MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : no
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : no
      Some remote MEP's MAC in error state         : yes # MAC Status Defects
yes/no
    Statistics:
      CCMs sent                                    : 1328
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
      LBRs received with corrupted data            : 0
      LBRs sent                                    : 0
      LTMs sent                                    : 0
      LTMs received                                : 0
      LTRs sent                                    : 0
      LTRs received                                : 0
      Sequence number of next LTM request          : 0
      1DMs sent                                    : 0
      Valid 1DMs received                          : 0
      Invalid 1DMs received                        : 0
      DMMs sent                                    : 0
      DMRs sent                                    : 0
      Valid DMRs received                          : 0
      Invalid DMRs received                        : 0
    Remote MEP count: 1
      Identifier    MAC address        State    Interface
        200     00:05:85:73:39:4a       ok    xe-5/0/0.0
```

Configuring Remote MEP Action Profile Support

Based on values of **interface-status-tlv** and **port-status-tlv** in the received CCM packets, a specific action, such as **interface-down**, can be taken using the **action-profile** options. Multiple action profiles can be configured on the router, but only one action profile can be assigned to a remote MEP.

The action profile can be configured with at least one event to trigger the action; but the action will be triggered if any one of these events occurs. It is not necessary for all of the configured events to occur to trigger **action**.

An action-profile can be applied only at the remote MEP level.

The following example shows an action profile configuration with explanatory comments added:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile tlv-action {
   event {
      # If interface status tlv with value specified in the config is received
      interface-status-tlv down|lower-layer-down;
      # If port status tlv with value specified in the config is received
      port-status-tlv blocked;
      # If connectivity is lost to the peer */
      adjacency-loss;
   }
   action {
      # Bring the interface down */
      interface-down;
   }
   default-actions interface-down;
   }
# domains
   maintenance-domain identifier {
      # maintenance domain level (0-7)
      level number;
      # association
      maintenance-association identifier {
         mep identifier {
            interface ge-x/y/z.w;
            remote-mep identifier {
               # Apply the action-profile for the remote MEP
               action-profile tlv-action;
            }
         }
      }
   }
```

Monitoring a Remote MEP Action Profile

You can use the **show oam ethernet connectivity-fault-management mep-database** command to view the action profile status of a remote MEP, as in the following example:

show oam ethernet connectivity-fault-management mep-database remote-mep

(Action Profile Event)

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5 remote-mep 200**

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none  # last status TLVs transmitted
 by the router
  Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 200, State: ok # displays the remote MEP name and state
    MAC address: 00:05:85:73:96:1f, Type: Configured
    Interface: ge-1/0/8.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: lower-layer-down
    Action profile: juniper  # displays remote MEP's action profile identifier
      Last event: Interface-status-tlv lower-layer-down  # last remote MEP event

                                                         # to trigger action
      Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
                              # action occurrence time
```

RELATED DOCUMENTATION

> *connectivity-fault-management*
>
> IEEE 802.1ag OAM Connectivity Fault Management Overview | **24**

Configuring Chassis ID TLV

In Release 16.1R2 and later, you can configure Junos OS to send the sender ID TLV along with the packets. The sender ID TLV is an optional TLV that is sent in continuity check messages (CCMs), loopback messages, and Link Trace Messages (LTMs), as specified in the IEEE 802.1ag standard. The sender ID TLV contains the chassis ID, which is the unique, CFM-based MAC address of the device, and the management IP address, which is an IPv4 or an IPv6 address.

The value of the **length** field in the TLV indicates whether or not the TLV contains the chassis ID information. The possible values for the **length** field are zero (**0**) or any valid number, which indicates the absence or presence of chassis ID information in the TLV, respectively.

You can enable Junos OS to send the sender ID TLV at the global level by using the **set protocols oam ethernet connectivity-fault-management sendid-tlv send-chassis-tlv** command. If the sender ID TLV is configured at the global level, then the default maintenance domain, maintenance association, and the maintenance association intermediate point (MIP) half function inherit this configuration.

You can also configure the sender ID TLV at the following hierarchy levels:

- **[edit protocols oam ethernet connectivity-fault-management]**.
- **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain-name* maintenance-association *maintenance-association-name* continuity-check]**.

The sender ID TLV configuration at the maintenance-association level takes precedence over the global-level configuration.

> **NOTE:** The sender ID TLV is supported only for 802.1ag PDUs and is not supported for performance monitoring protocol data units (PDUs).

SEE ALSO

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

Configuring MAC Flush Message Processing in CET Mode

In carrier Ethernet transport (CET) mode, MX Series routers are used as provider edge (PE) routers, and Nokia Siemens Networks A2200 Carrier Ethernet Switches (referred to as E-domain devices) that run standard-based protocols are used in the access side. On the MX Series routers, VPLS pseudowires are configured dynamically through label distribution protocol (LDP). On the E-domain devices, topology changes are detected through connectivity fault management (CFM) sessions running between the E-domain devices and the MX Series PE routers. The MX Series PE routers can bring the carrier Ethernet interface down if there is CFM connectivity loss. This triggers a local MAC flush as well as a targeted label distribution protocol (T-LDP) MAC flush notification that gets sent towards the remote MX Series PEs to trigger MAC flush on them.

In CET inter-op mode, MX Series routers need to interoperate with the Nokia Siemens Networks Ax100 Carrier Ethernet access devices (referred to as A-domain devices) that run legacy protocols. Nokia Siemens Networks A4100 and A8100 devices act as an intermediate between the MX Series PE routers and A-domain devices. These intermediate devices perform interworking function (IWF) procedures so that operations administration management (OAM) sessions can be run between MX Series routers and A-domain devices. There are no VPLS pseudowires between the MX Series PE routers and the Nokia Siemens Networks A4100 and A8100 intermediate devices, so there is no LDP protocol running between the PE routers to send topology change notifications. In order to communicate topology changes, MX Series routers can trigger a MAC flush and propagate it in the core. MX Series routers can use action profiles based upon the connection protection type length value (TLV) event. The action profile brings down the carrier edge logical interface in MX Series PE routers, which will trigger a local MAC flush and also propagate the topology change to the core using LDP notification.

For VPLS there is no end-to-end connectivity monitored. The access rings are independently monitored by running CFM down multiple end points (MEPs) on the working and protection paths for each of the services between the E-domain devices and the MX Series PE routers, and between the A-domain devices and the MX Series PE routers the IWF hosted by the Nokia Siemens Networks A-4100 devices. When there is a connectivity failure on the working path, the Nokia Siemens Networks Ax200 devices perform a switchover to the protection path, triggering a topology change notification (in the form of TLVs carried in CCM) to be sent on the active path.

Figure 10: CET inter-op Dual Homed Topology

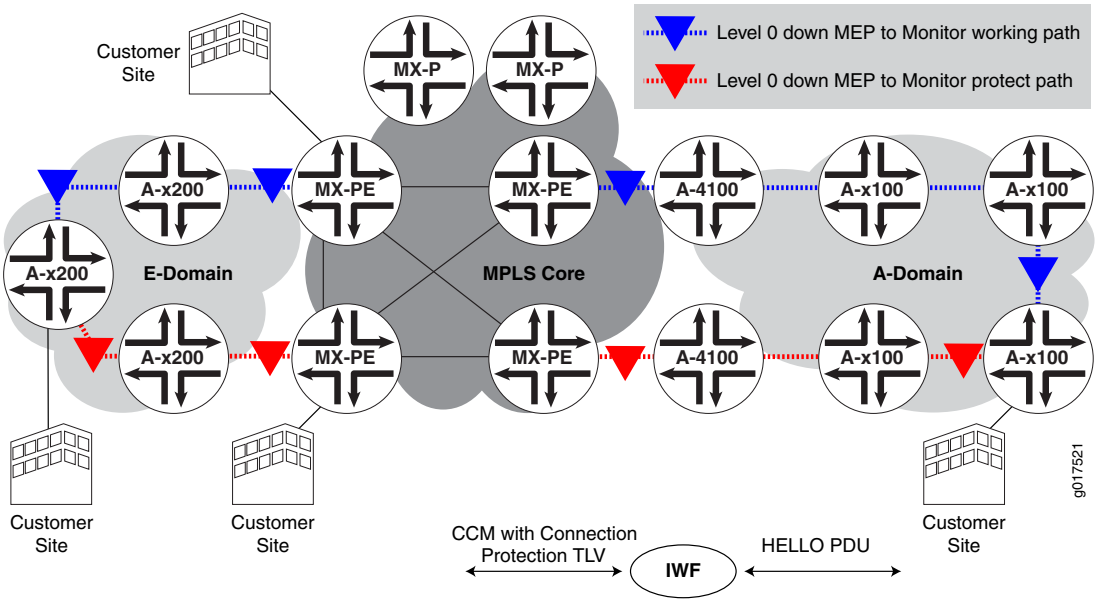


Figure 10 on page 119 describes the dual homed topology on MX Series PE routers connected to the A-domain. When an A-domain device triggers a switchover, it starts switching the service traffic to the new active path. This change is communicated in the HELLO protocol data units (PDUs) sent by that A-domain device on the working and protection paths. When the IWF in A4100 recieves these HELLO PDUs, it converts them to standard CCM messages and also inserts a connection protection TLV. The “Protection-in-use” field of the connection protection TLV is encoded with the currently active path, and is included in the CCM message. CCM messages are received by the MX Series PE routers through the VLAN spoke in A4100. In the above dual homed scenario, one MX Series PE router monitors the working path, and the other MX Series PE router monitors the protection path.

A MAC flush occurs when the CFM session that is monitoring the working path detects that the service traffic has moved to the protection path or when the CFM session that is monitoring the protection path detects that the service traffic has moved to the working path.

Figure 11: CET inter-op Dual Attached Topology

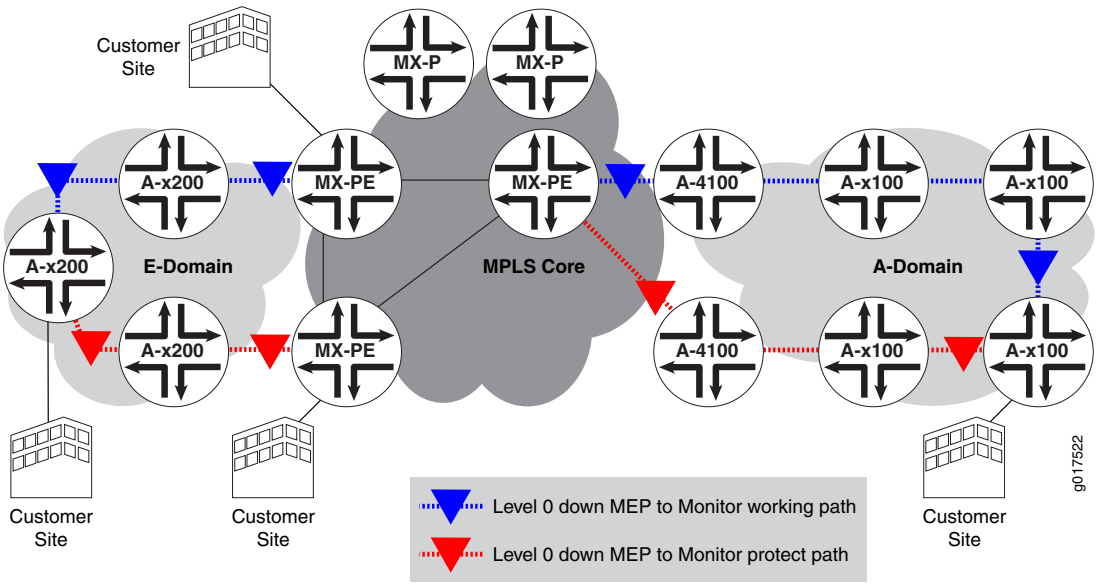


Figure 11 on page 120 describes the dual attached topology on MX Series PE routers connected to the A-domain. The MAC flush mechanism used in this case is also the same as the one used for the A-domain in the dual homed scenario (Figure 1). However in this case both the CFM sessions are hosted by only one MX Series PE router. When Ax100 in the A-domain detects topology changes, the MX Series PE router receives the connection protection TLV in the CCM message for the working and protection paths with the value of “Protection-in-use” indicating which path is the active one. Based upon the event that is generated for the CFM session, the MX Series PE router will bring down the appropriate interface which will trigger a local MAC flush.

Configuring a Connection Protection TLV Action Profile

An action profile can be configured to perform the **interface-down** action based on the values of **connection-protection-tlv** in the received CCM packets.

The following example shows an action profile configuration with explanatory comments added:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
   event {
      # If a connection protection TLV with a “Protection-in-use” value of SET is received */
      connection-protection-tlv <using-protection-path>;
      # If a connection protection TLV with a “Protection-in-use” value of RESET is received */
      connection-protection-tlv <using-working-path>;
   }
   action {
      # Bring the interface down */
      interface-down;
```

```
    }
}
```

SEE ALSO

connection-protection-tlv | 1776

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

Example: Configuring an Action Profile Based on Connection Protection TLVs

IN THIS SECTION

- Requirements | 121
- Overview and Topology | 121
- Configuration | 122

This example shows how to configure an action profile based on the connection protection TLV for the purposes of triggering MAC flushes based on topology changes in a CET network.

Requirements

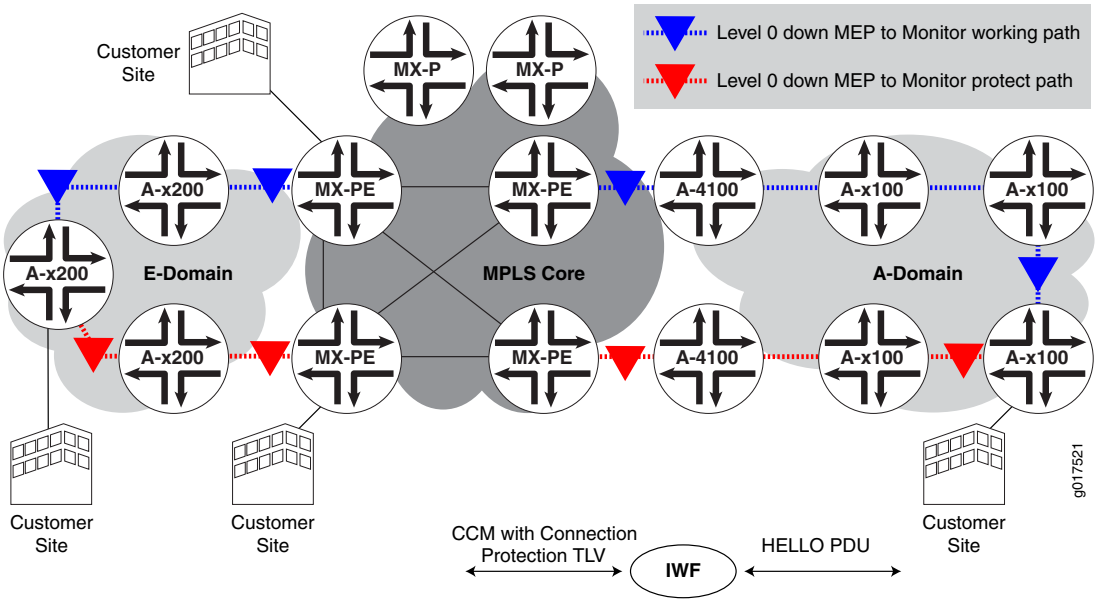
This example uses the following hardware and software components:

- Junos OS Release 11.2 or later
- A MX series PE router

Overview and Topology

The physical topology of a CET network using MX series PE routers is shown in Figure 12 on page 122

Figure 12: Topology of CET network



The following definitions describe the meaning of the device abbreviation and terms used in Figure 12 on page 122.

- Provider edge (PE) device—A device, or set of devices, at the edge of the provider network that presents the provider's view of the customer site.
- E-domain—Nokia Siemens Networks Carrier Ethernet Switches that run standard based protocols and are used in the access side.
- A-domain—Nokia Siemens Networks Carrier Ethernet Switches that run legacy protocols.

Configuration

Step-by-Step Procedure

To configure an action profile based on the connection protection TLV, preform these tasks:

1. Configure an action profile

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
   event {
```

2. If the connection protection TLV is received with a “Protection-in-use” value of SET, then the connection protection TLV should use the protection path

```
connection-protection-tlv <using-protection-path>;
```

3. If the connection protection TLV is received with a “Protection-in-use” value of RESET, then the connection protection TLV should use the working path

```
connection-protection-tlv <using-working-path>;
}
```

4. Configure the action profile to bring the interface down

```
action {
    /* Bring the interface down */
    interface-down;
}
}
```

Results

Check the results of the configuration

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
    event {
        connection-protection-tlv <using-protection-path>;
        connection-protection-tlv <using-working-path>;
    }
    action {
        interface-down;
    }
}
```

SEE ALSO

connection-protection-tlv | **1776**

Release History Table

Release	Description
17.3R1	Starting in Junos OS Release 17.3R1, you can enable connectivity fault management (CFM) monitoring between provider edge devices and customer edge devices when the customer edge device is not a Juniper device by using the remote defect indication (RDI) bit.
16.1	In Release 16.1R2 and later, you can configure Junos OS to send the sender ID TLV along with the packets.

RELATED DOCUMENTATION

Introduction to OAM Connectivity Fault Management (CFM) | 22

ITU-T Y.1731 Ethernet Service OAM Overview | 165

Configuring Continuity Check Messages

IN THIS SECTION

- Configuring Faster Protection Switching for Point-to-Point Network Topologies | 125
- Configuring Faster Convergence for Dual-Homed Multipoint-to-Multipoint Network Topologies | 127
- Configuring a Primary VLAN ID for Increased Flexibility | 128
- Configuring a Remote Maintenance Association to Accept a Different ID | 129

Junos OS provides enhancements to trigger faster protection-switching and convergence in the event of failures in Ethernet domains for Carrier Ethernet services. These enhancements can be used when CE devices in the Ethernet domain detect faster service failures and propagates the information in the interface-status TLV of the continuity-check messages (CCMs). When CCMs are received, PE devices can perform certain actions which facilitates faster protection-switching and convergence. You can configure CCM for better scalability using the information provided in this topic.

Configuring Faster Protection Switching for Point-to-Point Network Topologies

You can apply an action profile to provide faster protection switching for point-to-point network topologies with local switching configured. In a normal state, CCM sessions are configured on the working and protect interfaces. The CCM packets transmitted contain an interface-status TLV with the value up on the working interface and value down on the protect interface. When a link fails on the working interface, the protect interface starts receiving the interface-status TLV as up. With the profile configuration, if the interface-status TLV received on the protect interface is up, the working interface is automatically marked as **interface-down**.

To configure the **interface-status-tlv** down event, include the **interface-status-tlv down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure **interface-down** as the action profile's action, include the **interface-down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* action]** hierarchy level.

To configure *peer-interface* as the clear-action, include *peer-interface* at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* clear-action]** hierarchy level.

```
[edit protocols oam]
ethernet {
    connectivity-fault-management {
        action-profile p1 {
            event {
                interface-status-tlv down;
            }
            action {
                interface-down;
            }
            clear-action {
                interface-down peer-interface;
            }
        }
    }
}
```

In this action profile configuration, when the interface-status TLV is received as up, the *peer-interface* is marked as down.

The *peer-interface* is configured in the **protect-maintenance-association** statement. Consider the following example using the **protect-maintenance-association** statement in the configuration:

```
[edit protocols oam]
```

```
ethernet {
    connectivity-fault-management {
        action-profile p1 {
            event {
                adjacency-loss;
            }
            action {
                interface-down;
            }
            clear-action {
                interface-down peer-interface;
            }
        }
        maintenance-domain nsn {
            level 5;
            maintenance-association ma1 {
                protect-maintenance-association ma2;
                continuity-check {
                    interval 100ms;
                    connection-protection-tlv;
                }
                mep 100 {
                    interface ge-1/1/0.0;
                    direction down;
                    auto-discovery;
                }
            }
            maintenance-association ma2 {
                continuity-check {
                    interval 100ms;
                    connection-protection-tlv;
            }
            mep 101 {
                    interface ge-1/2/0.0;
                    direction down;
                    auto-discovery;
            }
            remote-mep 100
                action-profile p1;
            }
        }
    }
}
```

SEE ALSO

connectivity-fault-management

Configuring Faster Convergence for Dual-Homed Multipoint-to-Multipoint Network Topologies

You can apply an action profile to provide faster convergence for dual-homed multipoint-to-multipoint network topologies. If a multipoint-to-multipoint Ethernet service uses MAC-based forwarding and stale MAC addresses exist in the learning tables, this can result in traffic black holes in the network where incoming traffic is silently discarded, without informing the source that the data did not reach its intended recipient. With the profile configuration, if the interface-status TLV received on the protect interface is up, then the interface-status TLV on the working interface is marked as down and the PE device for the protect interface propagates a remote MAC-flush message to the PE devices in the virtual private LAN service (VPLS) by using TLDP-MAC-FLUSH. The MAC flush avoids traffic blackholing due to stale mac-db entries.

To configure the **interface-status-tlv** down event, include the **interface-status-tlv down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure **propagate-remote-flush** as the action profile's action, include the **propagate-remote-flush** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* action]** hierarchy level.

To configure **propagate-remote-flush** as the clear-action, include the **propagate-remote-flush** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* clear-action]** hierarchy level.

```
[edit protocols oam]
ethernet {
    connectivity-fault-management {
        action-profile test {
            event {
                interface-status-tlv down;
            }
            action {
                propagate-remote-mac-flush;
            }
            clear-action {
                propagate-remote-mac-flush;
            }
        }
    }
}
```

In this action profile configuration, when the incoming CCM packet contains the interface-status TLV with value down, the **propagate-remote-mac-flush** action is triggered for the action-profile.

SEE ALSO

> IEEE 802.1ag OAM Connectivity Fault Management Overview | 24
>
> *connectivity-fault-management*

Configuring a Primary VLAN ID for Increased Flexibility

You can assign a primary virtual LAN (VLAN) ID in the maintenance association for increased flexibility in the number of tags. When a **vlan-range** or **vlan-id-list** is configured on an interface, the service OAM must run on one of the VLANs. The VLAN assigned for service monitoring is considered the primary VLAN. If a **primary-vid** is not configured, Junos OS assigns the first VLAN from the **vlan-range** or **vlan-id-list**. In earlier releases, Junos OS assigned VLAN 4095.

To configure a primary VLAN ID, you can specify the **primary-vid** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name*]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management]
maintenance domain md3 {
   level 3;
   maintenance-association ma3 {
      primary-vid 2000;
      continuity-check {
         interval 10ms;
         connection-protection-tlv;
      }
      mep 2 {
         interface ge-2/2/0.0;
         direction up;
         auto-discovery;
      }
   }
}
```

SEE ALSO

> IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

connection-protection-tlv | 1776

connectivity-fault-management

Configuring a Remote Maintenance Association to Accept a Different ID

You can configure a maintenance association to accept a different maintenance association identifier (ID) from a neighbor by including a **remote-maintenance-association** statement. The 802.1ag CCM sessions expect the same maintenance association identifier from its neighbors. If there is a maintenance association identifier mismatch, the PDUs are marked as error PDUs. If a **remote-maintenance-association** statement is configured, a different maintenance association identifier is accepted and the 802.1ag CCM sessions do not mark the CCM PDUs as error PDUs when the maintenance-association name is the same as the name specified in the **remote-maintenance-association** statement.

To configure a remote maintenance association, include the **remote-maintenance-association** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name*]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management]
maintenance domain md3 {
   level 1;
   maintenance-association ma3 {
      remote-maintenance-association fix-ma;
      continuity-check {
         interval 10ms;
         connection-protection-tlv;
      }
      mep 2 {
         interface ge-2/2/0.0;
         direction up;
         auto-discovery;
      }
   }
}
```

Using this configuration, interoperability is improved for CCMs with low-end CE devices supporting fixed maintenance association identifier configurations.

SEE ALSO

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

connectivity-fault-management

connection-protection-tlv | 1776

RELATED DOCUMENTATION

Introduction to OAM Connectivity Fault Management (CFM) | 22

Configuring Connectivity Fault Management (CFM) | 29

CHAPTER 4

Link Fault Management for Routers

IN THIS CHAPTER

- Introduction to OAM Link Fault Management (LFM) | 131
- Configuring Link Fault Management | 136
- Remote Fault Detection for Link Fault Management | 154
- Remote Loopback for Link Fault Management | 156

Introduction to OAM Link Fault Management (LFM)

IN THIS SECTION

- IEEE 802.3ah OAM Link-Fault Management Overview | 131
- Understanding Ethernet OAM Link Fault Management for ACX Series Routers | 132
- Configuring Ethernet 802.3ah OAM | 134

Use this topic to understand more about link fault management (LFM) and how to configure link fault management.

IEEE 802.3ah OAM Link-Fault Management Overview

Ethernet interfaces capable of running at 100 Mbps or faster on EX Series switches, PTX Series, MX Series, M Series (except M5 and M10 routers), and T Series routers support the IEEE 802.3ah standard for Operation, Administration, and Management (OAM). You can configure IEEE 802.3ah OAM on Ethernet point-to-point direct links or links across Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities as Ethernet moves from being solely an enterprise technology to being a WAN and access technology, as well as being backward-compatible with existing Ethernet technology. Junos OS supports IEEE 802.3ah link-fault management.

The features of link-fault management are:

- Discovery
- Link monitoring
- Remote fault detection
- Remote loopback

Starting in Junos OS Release 17.3R1, the Ethernet link fault management daemon (lfmd) runs on the backup Routing Engine as well when graceful Routing Engine switchover (GRES) is configured.

The following features are not supported:

- Ethernet running on top of a Layer 2 protocol, such as Ethernet over ATM, is not supported in OAM configurations.
- Remote loopback is not supported on the 10-Gigabit Ethernet LAN/WAN PIC with SFP+.
- The remote loopback feature mentioned in section 57.2.11 of IEEE 802.3ah is not supported on T4000 routers.

NOTE: Aggregated Ethernet member links will now use the physical MAC address as the source MAC address in 802.3ah OAM packets.

SEE ALSO

Detecting Remote Faults | 154

Enabling Nonstop Routing for Ethernet Link Fault Management on Backup Routers | 158

Understanding Ethernet OAM Link Fault Management for ACX Series Routers

The Juniper Networks Junos operating system (Junos OS) for Juniper Networks ACX Series routers allows the Ethernet interfaces on these routers to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward compatible with the existing Ethernet technology.

Ethernet OAM provides tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual LAN identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports or a virtual service such as a pseudowire.
- Isolate faults over a flat (or single-operator) network architecture or nested or hierarchical (or multiprovider) networks.

The following OAM LFM features are supported on ACX Series routers:

- Discovery and Link Monitoring

  The discovery process is triggered automatically when OAM is enabled on the interface. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard. You can specify the discovery mode used for IEEE 802.3ah OAM support. 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. After the discovery process has been initiated, both sides participate in the process. The router performs link monitoring by sending periodic OAM protocol data units (PDUs) to advertise OAM mode, configuration, and capabilities.

  You can specify the number of OAM PDUs that an interface can skip before the link between peers is considered down.

- Remote Fault Detection

  Remote fault detection uses flags and events. Flags are used to convey the following:

  - **Link Fault** means a loss of signal
  - **Dying Gasp** means an unrecoverable condition such as a power failure. In this condition, the local peer informs the remote peer about the failure state. When the remote peer receives a dying-gasp PDU, it takes an action corresponding to the action profile configured with the **link-adjacency-loss** event.

    NOTE: ACX5096 and ACX5048 routers do not support dying-gasp.

    ACX Series routers can generate and receive dying-gasp packets. When LFM is configured on an interface, a dying-gasp PDU is generated for the interface on the following failure conditions:

    - Power failure
    - Packet Forwarding Engine panic or a crash

  - **Critical Event** means an unspecified vendor-specific critical event.

  You can specify the interval at which OAM PDUs are sent for fault detection.

NOTE: ACX Series routers support the receipt of dying-gasp packets, but cannot generate them.

- Remote Loopback Mode

  Remote loopback mode ensures link quality between the router and a remote peer during installation or troubleshooting. In this mode, when the interface receives a frame that is not an OAM PDU or a PAUSE frame, it sends it back on the same interface on which it was received. The link appears to be in the active state. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.

  If a remote data terminal equipment (DTE) supports remote loopback mode, Junos OS can place the remote DTE into loopback mode. When you place a remote DTE into loopback mode, the interface receives the remote loopback request and puts the interface into remote loopback mode. When the interface is in remote loopback mode, all frames except OAM PDUs and PAUSE frames are looped back. No changes are made to the frames. OAM PDUs continue to be sent and processed.

SEE ALSO

Remote Fault Detection for Link Fault Management | 154

Configuring Ethernet 802.3ah OAM

The IEEE 802.3ah standard for Operation, Administration, and Management (OAM) provides a specification for *Ethernet in the first mile (EFM)* connectivity. EFM defines how Ethernet can be transmitted over new media types using new Ethernet physical layer (PHY) interfaces. You can configure IEEE 802.3ah OAM on Ethernet point-to-point direct links or links across Ethernet repeaters. The IEEE 802.3ah OAM standard meets the requirement for OAM capabilities as Ethernet moves from being solely an enterprise technology to being a WAN and access technology, as well as being backward-compatible with existing Ethernet technology.

For Ethernet interfaces capable of running at 100 Mbps or faster, the IEEE 802.3ah OAM standard is supported on numerous Juniper Networks routers and switches. This topic describes configuration support for IEEE 802.3ah OAM features on routers.

Beginning in Junos OS Release 12.1, PTX Series routers support the following IEEE 802.3ah OAM features at the physical interface level:

- Discovery and link monitoring
- Fault signaling and detection
- Periodic packet management (PPM) processing

- Action profile support
- Graceful Routing Engine switchover (GRES)

To configure 802.3ah OAM support for Ethernet interfaces, include the **oam** statement at the **[edit protocols]** hierarchy level:

```
oam {
    ethernet {
        link-fault-management {
            interfaces {
                interface-name {
                    pdu-interval interval;
                    link-discovery (active | passive);
                    pdu-threshold count;
                }
            }
        }
    }
}
```

You can configure threshold values for fault events that trigger the sending of link event TLVs when the values exceed the threshold. To set threshold values for fault events on an interface, include the **event-thresholds** statement at the **[edit protocols oam ethernet link-fault-management interface]** hierarchy level.

You can also configure OAM threshold values within an action profile and apply the action profile to multiple interfaces. To create an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level.

You can configure Ethernet OAM either on an aggregate interface or on each of its member links. However, we recommend that you configure Ethernet OAM on the aggregate interface, and this will internally enable Ethernet OAM on the member links.

To view OAM statistics, use the **show oam ethernet link-fault-management** operational mode command. To clear OAM statistics, use the **clear oam ethernet link-fault-management statistics** operational mode command. To clear link-fault management state information and restart the link discovery process on Ethernet interfaces, use the **clear oam ethernet link-fault-management state** operational mode command. For more information about these commands, see the CLI Explorer.

To enable IEEE 802.3ah OAM support, include the **interface** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level:

```
[edit protocols oam ethernet link-fault-management interface interface-name]
```

When you enable IEEE 802.3ah OAM on a physical interface, the discovery process is automatically triggered.

SEE ALSO

- event-thresholds | 1879
- action-profile | 1757

Release History Table

Release	Description
17.3R1	Starting in Junos OS Release 17.3R1, the Ethernet link fault management daemon (lfmd) runs on the backup Routing Engine as well when graceful Routing Engine switchover (GRES) is configured.

RELATED DOCUMENTATION

- Remote Fault Detection for Link Fault Management | 154
- Remote Loopback for Link Fault Management | 156

Configuring Link Fault Management

IN THIS SECTION

- Configuring Link Discovery | 137
- Configuring the OAM PDU Interval | 138
- Configuring the OAM PDU Threshold | 138
- Configuring Threshold Values for Local Fault Events on an Interface | 138
- Disabling the Sending of Link Event TLVs | 139
- Example: Configuring IEEE 802.3ah OAM Support on an Interface | 139
- Example: Configuring IEEE 802.3ah OAM Support for an Interface on ACX Series | 140
- Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge | 143
- Example: Configuring Ethernet LFM for CCC | 145
- Example: Configuring Ethernet LFM for Aggregated Ethernet | 146

- Configuring an OAM Action Profile | **149**
- Specifying the Actions to Be Taken for Link-Fault Management Events | **150**
- Monitoring the Loss of Link Adjacency | **151**
- Monitoring Protocol Status | **152**
- Configuring Threshold Values for Fault Events in an Action Profile | **153**
- Applying an Action Profile | **153**

Use this topic to understand how to configure link fault management features on your device. You can also use this topic to configure an action profile to specify the LFM action that must be performed when a specific LFM event occurs and apply the action profile.

Configuring Link Discovery

When the IEEE 802.3ah OAM protocol is enabled on a physical interface, the discovery process is automatically triggered. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard.

You can specify the discovery mode used for IEEE 802.3ah OAM support. The discovery process is triggered automatically when OAM IEEE 802.3ah functionality is enabled on a port. Link monitoring is done when the interface sends periodic OAM PDUs.

To configure the discovery mode, include the **link-discovery** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
link-discovery (active | passive);
```

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. After the discovery process has been initiated, both sides participate in discovery.

SEE ALSO

link-discovery

Configuring the OAM PDU Interval

Periodic OAM PDUs are sent to perform link monitoring.

You can specify the periodic OAM PDU sending interval for fault detection.

To configure the sending interval, include the **pdu-interval** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
pdu-interval interval;
```

The periodic OAM PDU interval range is from 100 through 1000 milliseconds. The default sending interval is 1000 milliseconds.

SEE ALSO

pdu-interval | 1906

Configuring the OAM PDU Threshold

You can specify the number of OAM PDUs that an interface can miss before the link between peers is considered down.

To configure the number of PDUs that can be missed from the peer, include the **pdu-threshold** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
pdu-threshold threshold-value;
```

The threshold value range is from 3 through 10. The default is three PDUs.

SEE ALSO

pdu-threshold | 1907

Configuring Threshold Values for Local Fault Events on an Interface

You can configure threshold values on an interface for the local errors that trigger the sending of link event TLVs.

To set the error threshold values for sending event TLVs, include the **frame-error**, **frame-period**, **frame-period-summary**, and **symbol-period** statements at the **[edit protocols oam ethernet link-fault-management interface *interface-name* event-thresholds]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

SEE ALSO

- event-thresholds | **1879**
- *frame-error*
- frame-period | **1883**
- frame-period-summary | **1885**
- *symbol-period*

Disabling the Sending of Link Event TLVs

You can disable the sending of link event TLVs.

To disable the monitoring and sending of PDUs containing link event TLVs in periodic PDUs, include the **no-allow-link-events** statement at the **[edit protocols oam ethernet link-fault-management interface *interface-name* negotiation-options]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name negotiation-options]
no-allow-link-events;
```

SEE ALSO

- *no-allow-link-events*

Example: Configuring IEEE 802.3ah OAM Support on an Interface

Configure 802.3ah OAM support on a 10-Gigabit Ethernet interface:

```
[edit]
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface xe-0/0/0 {
                    link-discovery active;
                    pdu-interval 800;
                    pdu-threshold 4;
                    remote-loopback;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                    event-thresholds {
                        frame-error 30;
                        frame-period 50;
                        frame-period summary 40;
                        symbol-period 20;
                    }
                }
            }
        }
    }
}
```

SEE ALSO

link-fault-management

Example: Configuring IEEE 802.3ah OAM Support for an Interface on ACX Series

Junos OS for ACX Series routers allows the Ethernet interfaces on these routers to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example describes how to enable and configure OAM on a Gigabit Ethernet interface.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2 or later for ACX Series routers.

- An ACX1000 or ACX2000 router.

Overview and Topology

In this example, you configure a 10-Gigabit Ethernet interface on an ACX Series router with 802.3ah OAM support, which includes: link discovery, protocol data units (PDUs), remote loopback, negotiation, and event thresholds.

Configuring IEEE 802.3ah OAM on an ACX Series Router

CLI Quick Configuration

To quickly configure IEEE 802.3ah Ethernet OAM, copy the following commands and paste them into the CLI:

```
edit
edit protocols oam ethernet link-fault-management
set interface xe-0/0/0 link-discovery active pdu-interval 800 pdu-threshold 4 remote-loopback negotiation-options
    allow-remote-loopback
set interface xe-0/0/0 event-thresholds frame-error 30 frame-period 50 frame-period-summary 40 symbol-period
    20
```

Step-by-Step Procedure

To configure IEEE 802.3ah OAM support on an interface:

1. Enable IEEE 802.3ah OAM support on an interface:

   ```
   [edit protocols oam ethernet link-fault-management]
   ```

   user@router1# **set** interface (OAM Link-Fault Management) **xe-0/0/0**

2. Specify that the interface initiates the discovery process by setting the link discovery mode to **active**:

   user@router# **set interface xe-0/0/0** ***link-discovery*** **active**

3. Set the periodic OAM PDU-sending interval (in milliseconds) to 800:

   user@router# **set interface xe-0/0/0** pdu-interval **800**

4. Define the number of OAM PDUs to miss before an error is logged as 4:

   user@router# **set interface xe-0/0/0** pdu-threshold **4**

5. Configure the remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes:

   user@router# **set interface xe-0/0/0** ***remote-loopback***

6. Configure remote loopback support for the local interface:

   user@router# **set interface xe-0/0/0 *negotiation-options allow-remote-loopback***

7. Set the threshold count for sending frame error events to 30:

   user@router# **set interface xe-0/0/0 event-thresholds *frame-error* 30**

8. Set the threshold count for sending frame period error events to 50:

   user@router# **set interface xe-0/0/0 event-thresholds frame-period 50**

9. Configure the threshold count for sending frame period summary error events to 40:

   user@router# **set interface xe-0/0/0 event-thresholds frame-period-summary 40**

10. Set the threshold count for sending symbol period events to 20:

    user@router# **set interface xe-0/0/0 event-thresholds *symbol-period* 20**

Results

Check the results of the configuration:

```
[edit]
user@router# show
```

```
[edit]
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface xe-0/0/0 {
                    link-discovery active;
                    pdu-interval 800;
                    pdu-threshold 4;
                    remote-loopback;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                    event-thresholds {
                        frame-error 30;
                        frame-period 50;
                        frame-period-summary 40;
                        symbol-period 20;
```

```
            }
          }
        }
      }
    }
  }
```

SEE ALSO

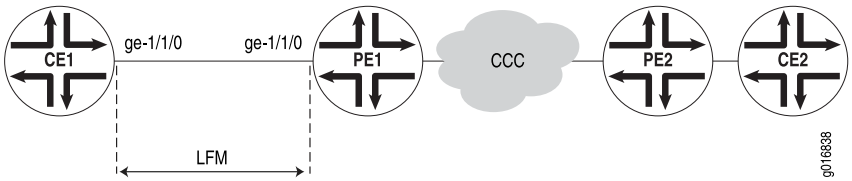
link-fault-management

Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge

In this example, LFM is enabled on an IP link between the provider edge (PE) and customer edge (CE) interfaces. If the link goes down, the fault will be detected by LFM and the interfaces on both sides will be marked **Link-Layer-Down**. This results in notifications to various subsystems (for example, routing) which will take appropriate action.

The link running LFM is shown in Figure 13 on page 143.

Figure 13: Ethernet LFM Between Provider Edge and Customer Edge



To configure Ethernet LFM on an IP link between PE and CE interfaces:

1. Configure LFM on the PE router:

```
[edit]
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
```

```
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

2. Configure LFM on the CE router:

```
[edit]
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

SEE ALSO

Ethernet Interfaces User Guide for Routing Devices

IEEE 802.3ah OAM Link-Fault Management Overview | **131**

Example: Configuring Ethernet LFM for CCC | **145**

Example: Configuring Ethernet LFM for Aggregated Ethernet | **146**

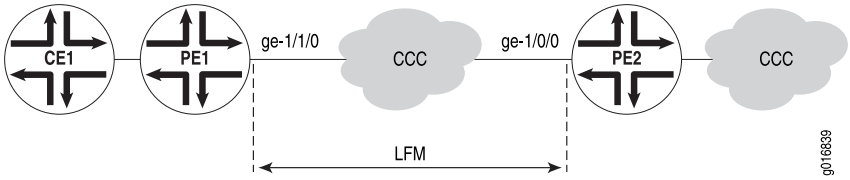
Example: Configuring Ethernet LFM with Loopback Support | 162

Example: Configuring Ethernet LFM for CCC

In this example, LFM is configured between two PEs (PE1 and PE2) connected using CCC. With LFM in place, a link fault will be detected immediately, instead of depending on routing protocols to find the fault on end-to-end CCC connection. This also helps in detecting the exact failed link instead of only finding that the end-to-end CCC connectivity has failed. Also, because LFM runs at the link-layer level, it does not need a IP address to operate and so can be used where bidirectional fault detection (BFD) cannot.

The links running LFM are shown in Figure 14 on page 145

Figure 14: Ethernet LFM for CCC



To configure Ethernet LFM between two PEs connected using CCC:

1. Configure LFM on the PE1 router with CCC:

```
[edit]
interfaces ge-1/1/0 {
    encapsulation ethernet-ccc;
    unit 0;
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

2. Configure LFM on the PE2 router with CCC:

```
[edit]
interfaces ge-1/0/0 {
    encapsulation ethernet-ccc;
    unit 0;
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/0/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

SEE ALSO

Ethernet Interfaces User Guide for Routing Devices

IEEE 802.3ah OAM Link-Fault Management Overview | **131**

Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge | **143**

Example: Configuring Ethernet LFM for Aggregated Ethernet | **146**

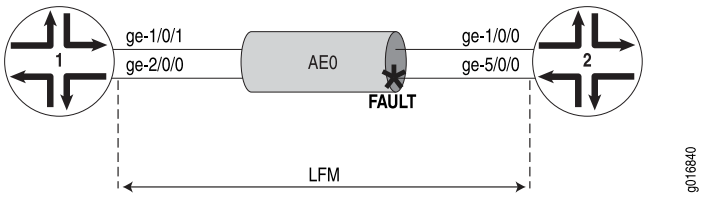
Example: Configuring Ethernet LFM with Loopback Support | **162**

Example: Configuring Ethernet LFM for Aggregated Ethernet

In this example, LFM is configured on an aggregated Ethernet interface (AE0) between Router 1 and Router 2. When configured on aggregated Ethernet, LFM runs on all the individual member links. LFM is enabled or disabled on the member links as they are added or deleted from the aggregation group. The status of individual links is used to determine the status of the aggregated interface.

The use of LFM with aggregated Ethernet is shown in Figure 15 on page 147.

Figure 15: Ethernet LFM for Aggregated Ethernet



To configure LFM on an aggregated Ethernet interface between two routers:

1. Configure LFM on Router 1 for AE0:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 1;
        }
    }
}
interfaces ge-1/0/1 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ge-2/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ae0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ae0;
            }
        }
    }
```

```
}
```

2. Configure LFM on Router 2 for AE0:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 1;
        }
    }
}
interfaces ge-1/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ge-5/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ae0 {
    unit 0 {
        family inet {
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ae0;
            }
        }
    }
}
```

SEE ALSO

Ethernet Interfaces User Guide for Routing Devices

IEEE 802.3ah OAM Link-Fault Management Overview | **131**

Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge | **143**

Example: Configuring Ethernet LFM for CCC | **145**

Example: Configuring Ethernet LFM with Loopback Support | **162**

Configuring an OAM Action Profile

You can create an action profile to define event fault flags and thresholds and the action to be taken. You can then apply the action profile to one or more interfaces.

To configure an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level:

```
action-profile profile-name {
    action {
        syslog;
        link-down;
        send-critical-event;
    }
    event {
        link-adjacency-loss;
        link-event-rate {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
        protocol-down;
    }
}
```

NOTE: Starting from Junos OS Release 14.2, whenever link-fault management (LFM) with an action profile is configured to mark the interface as down (by including the link-down statement at the [edit protocols oam ethernet link-fault-management] hierarchy level), the port is placed in the blocked state (STP state). In such a state of the interface, data traffic is not transmitted out on that interface. Because the connectivity-fault management (CFM) downstream maintenance MEPs come up on blocked ports, the CFM sessions come up properly. However, the interface is down and the interface status TLV does not contain the correct status. Only if you configure the port status TLV, the actual status of the port is reflected. The interface status TLV does not carry the actual state of the port.

SEE ALSO

Setting a Remote Interface into Loopback Mode | 156

Enabling Remote Loopback Support on the Local Interface | 157

Specifying the Actions to Be Taken for Link-Fault Management Events

You can specify the action to be taken by the system when the configured link-fault event occurs. Multiple action profiles can be applied to a single interface. For each action-profile, at least one event and one action must be specified. The actions are taken only when all of the events in the action profile are true. If more than one action is specified, all the actions are executed.

You might want to set a lower threshold for a specific action such as logging the error and set a higher threshold for another action such as sending a critical event TLV.

To specify the action, include the **action** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]
event {
    link-adjacency-loss;
    protocol-down;
}
action {
    syslog;
    link-down;
    send-critical-event;
}
```

To create a system log entry when the link-fault event occurs, include the **syslog** statement.

To administratively disable the link when the link-fault event occurs, include the **link-down** statement.

To send IEEE 802.3ah link event TLVs in the OAM PDU when a link-fault event occurs, include the **send-critical-event** statement.

> **NOTE:** If multiple actions are specified in the action profile, all of the actions are executed in no particular order.

SEE ALSO

- action | **1852**
- syslog | **1916**
- *link-down*
- send-critical-event | **1913**

Monitoring the Loss of Link Adjacency

You can specify actions be taken when link adjacency is lost. When link adjacency is lost, the system takes the action defined in the **action** statement of the action profile.

To configure the system to take action when link adjacency is lost, include the **link-adjacency-loss** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]
link-adjacency-loss;
```

SEE ALSO

- *link-adjacency-loss*
- Enabling Remote Loopback Support on the Local Interface | **157**

Monitoring Protocol Status

The CCC-DOWN flag is associated with a circuit cross-connect (CCC) connection, Layer 2 circuit, and Layer 2 VPN, which send the CCC-DOWN status to the kernel. The CCC-DOWN flag indicates that the CCC is down. The CCC-DOWN status is sent to the kernel when the CCC connection, Layer 2 circuit, or Layer 2 VPN is down. This in turn, brings down the CE-facing PE interface associated with the CCC connection, Layer 2 circuit, or Layer 2 VPN.

When the CCC-DOWN flag is signaled to the IEEE 802.3ah protocol, the system takes the action defined in the **action** statement of the action profile. For additional information about Layer 2 circuits, see the Junos OS Layer 2 Circuits User Guide, Junos OS VPNs Configuration Guide.

To monitor the IEEE 802.3ah protocol, on the CE-facing PE interface, include the **protocol-down** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

1. In configuration mode, go to the **[edit protocols oam ethernet link-fault-management action-profile profile-name event]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet link-fault-management action-profile profile-name event
```

2. Include the **protocol-down** statement.

```
[edit protocols oam ethernet link-fault-management action-profile profile-name event]
user@host# set protocol-down
```

NOTE: If multiple events are specified in the action profile, all the events must occur before the specified action is taken.

SEE ALSO

protocol-down | 1910

Setting a Remote Interface into Loopback Mode | 156

Enabling Remote Loopback Support on the Local Interface | 157

Configuring Threshold Values for Fault Events in an Action Profile

You can configure link event thresholds for received error events that trigger the action specified in the **action** statement. You can then apply the action profile to one or more interfaces.

To configure link event thresholds, include the **link-event-rate** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

```
link-event-rate {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

SEE ALSO

link-event-rate

Applying an Action Profile

You can apply an action profile to one or more interfaces.

To apply an action profile to an interface, include the **apply-action-profile** statement at the **[edit protocols oam ethernet link-fault-management action-profile interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
apply-action-profile profile-name;
```

SEE ALSO

apply-action-profile | 1859

Release History Table

Release	Description
14.2	Starting from Junos OS Release 14.2

RELATED DOCUMENTATION

Remote Loopback for Link Fault Management | 156

Remote Fault Detection for Link Fault Management

IN THIS SECTION

Detecting Remote Faults | 154
Enabling Dying Gasp Functionality | 155

Use this topic to understand more about remote faults and how they are detected and also how to enable the dying gasp feature to avoid file system corruption for LFM.

Detecting Remote Faults

Fault detection is either based on flags or fault event type, length, and values (TLVs) received in OAM protocol data units (PDUs). Flags that trigger a link fault are:

- Critical Event
- Dying Gasp
- Link Fault

The link event TLVs are sent by the remote DTE by means of event notification PDUs. Link event TLVs are:

- Errored Symbol Period Event
- Errored Frame Event
- Errored Frame Period Event
- Errored Frame Seconds Summary Event

SEE ALSO

IEEE 802.3ah OAM Link-Fault Management Overview | 131

Configuring IEEE 802.3ah OAM Link-Fault Management

Enabling Dying Gasp Functionality

Dying gasp means an unrecoverable condition such as a power failure. In this condition, the local peer informs the remote peer about the failure state. When the remote peer receives a dying-gasp PDU, it takes an action corresponding to the action profile configured with the **link-adjacency-loss** event. Dying gasp helps to avoid file system corruption.

> **NOTE:** ACX5096 and ACX5048 routers do not support dying-gasp.

ACX Series routers can generate and receive dying-gasp packets. When LFM is configured on an interface, a dying-gasp PDU is generated for the interface on the following failure conditions:

- Power failure
- Packet Forwarding Engine panic or a crash

ACX Series routers support the following CLI statements to enable dying-gasp functionality:

- **dgasp-int**—Enables dying-gasp functionality.
- **dgasp-usb**—Resets USB port during dying-gasp event.

The **dgasp-int** and **dgasp-usb** CLI statements are added under the **[edit system]** hierarchy to enable dying-gasp functionality.

To enable dying-gasp functionality, you need to configure the **dgasp-int** and **dgasp-usb** CLI statements as shown below:

```
root@host% cli
root@host> configure
Entering configuration mode

[edit]
root@host# set system dgasp-int

[edit]
root@host# set system dgasp-usb

[edit]
root@host# commit

commit complete

[edit]
root@host# show system
```

```
dgasp-int;
dgasp-usb;
```

The dying-gasp functionality is disabled by default.

SEE ALSO

- Understanding Ethernet OAM Link Fault Management for ACX Series Routers | 132

RELATED DOCUMENTATION

- Introduction to OAM Link Fault Management (LFM) | 131

Remote Loopback for Link Fault Management

IN THIS SECTION

- Setting a Remote Interface into Loopback Mode | 156
- Enabling Remote Loopback Support on the Local Interface | 157
- Enabling Nonstop Routing for Ethernet Link Fault Management on Backup Routers | 158
- Example: Configuring Ethernet LFM with Loopback Support | 162

Use this topic to understand what happens when you set a remote interfaces in loopback mode and how to enable remote loopback. You can also learn how to enable nonstop routing for LFM.

Setting a Remote Interface into Loopback Mode

You can configure the software to set the remote DTE into loopback mode on the following interfaces:

- IQ2 and IQ2-E Gigabit Ethernet interfaces
- Ethernet interfaces on the MX Series routers or EX Series switches

Junos OS can place a remote DTE into loopback mode (if remote-loopback mode is supported by the remote DTE). When you place a remote DTE into loopback mode, the interface receives the remote-loopback

request and puts the interface into remote-loopback mode. When the interface is in remote-loopback mode, all frames except OAM PDUs are looped back without any changes made to the frames. OAM PDUs continue to be sent to the management plane and processed.

To configure remote loopback, include the **remote-loopback** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]
remote-loopback;
```

To take the remote DTE out of loopback mode, remove the **remote-loopback** statement from the configuration.

SEE ALSO

remote-loopback

Enabling Remote Loopback Support on the Local Interface

You can allow a remote DTE to set a local interface into remote loopback mode on IQ2 and IQ2-E Gigabit Ethernet interfaces and all Ethernet interfaces on the MX Series routers and EX Series switches. When a remote-loopback request is sent by a remote DTE, the Junos OS places the local interface into loopback mode. When an interface is in loopback mode, all frames except OAM PDUs are looped back without any changes to the frames. OAM PDUs continue to be sent to the management plane and processed. By default, the remote loopback feature is not enabled.

To enable remote loopback, include the **allow-remote-loopback** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name* negotiation-options]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name negotiation-options]
allow-remote-loopback;
```

NOTE: Activation of OAM remote loopback may result in data frame loss.

SEE ALSO

allow-remote-loopback

Enabling Nonstop Routing for Ethernet Link Fault Management on Backup Routers

Starting in Junos OS Release 17.3R1, the Ethernet link fault management daemon (lfmd) runs on the backup Routing Engine as well when graceful Routing Engine switchover (GRES) is configured. When the lfmd daemon runs on the backup Routing Engine as well, the link fault management states are kept in sync and so minimal effort is required by the lfmd daemon post switch over.

To enable Nonstop routing for Ethernet LFM on backup routers:

1. Enable graceful Routing Engine switchover. By default, GRES is disabled. To enable GRES, include the **graceful-switchover** statement at the [**edit chassis redundancy**] hierarchy level. By default, Nonstop routing is disabled. When you enable GRES, NSR is enabled.

   ```
   [edit chassis redundancy]
   user@host# set graceful-switchover
   ```

2. Synchronize the Routing Engine configuration. To synchronize the master Routing Engine configuration with the backup, include the **synchronize** statement at the [**edit system**] hierarchy level.

   ```
   [edit system]
   user@host# set commit synchronize
   ```

3. After enabling nonstop routing, commit the configuration.

   ```
   [edit routing options]
   user@host# commit
   ```

4. To verify if nonstop routing is enabled on the backup router, at the operational mode, use the **show oam ethernet link-fault-management** command on the master router and then the backup router. Because you have enabled synchronization, the output of the master router and the backup router is identical. However, the statistics maintained by the master router are not synchronized with the backup router..

   ```
   {master}
   user@host# show oam ethernet link-fault-management ge-0/2/0 detail
   ```

   ```
   Interface: ge-0/2/0
       Status: Running, Discovery state: Send Any
       Transmit interval: 100ms, PDU threshold: 3 frames, Hold time: 300ms
       Peer address: ac:4b:c8:81:90:a4
   ```

```
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 786, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Enabled, Loop status: Not Found
    Detect LOC: Enabled, LOC status: Not Found
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                   Invoked     Executed
  LK_ADJ_LOSS100_1                         1        1
  LK_ADJ_LOSS100_2                         1        0
```

```
  LK_ADJ_LOSS100_3                        1        0
  LK_ADJ_LOSS101_1                        1        1
  LK_ADJ_LOSS101_2                        1        0
  LK_ADJ_LOSS101_3                        1        0
  LK_ADJ_LOSS106_1                        0        0
  LK_ADJ_LOSS106_2                        0        0
  LK_ADJ_LOSS106_3                        0        0
  LK_ADJ_LOSS107_1                        0        0
  LK_ADJ_LOSS107_2                        0        0
  LK_ADJ_LOSS107_3                        0        0
```

{backup}
user@host# show oam ethernet link-fault-management ge-0/2/0 detail

```
Interface: ge-0/2/0
    Status: Running, Discovery state: Send Any
    Transmit interval: 100ms, PDU threshold: 3 frames, Hold time: 300ms
    Peer address: ac:4b:c8:81:90:a4
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 786, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
```

```
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Enabled, Loop status: Not Found
    Detect LOC: Enabled, LOC status: Not Found
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                    Invoked     Executed
  LK_ADJ_LOSS100_1                          0        0
  LK_ADJ_LOSS100_2                          0        0
  LK_ADJ_LOSS100_3                          0        0
  LK_ADJ_LOSS101_1                          0        0
  LK_ADJ_LOSS101_2                          0        0
  LK_ADJ_LOSS101_3                          0        0
  LK_ADJ_LOSS106_1                          0        0
  LK_ADJ_LOSS106_2                          0        0
  LK_ADJ_LOSS106_3                          0        0
  LK_ADJ_LOSS107_1                          0        0
  LK_ADJ_LOSS107_2                          0        0
  LK_ADJ_LOSS107_3                          0        0
```

NOTE: After the switchover, if issues are observed, use the **clear oam ethernet link-fault-management state** command for specific sessions. If the issue does not get resolved, restart the lfmd daemon.

SEE ALSO

IEEE 802.3ah OAM Link-Fault Management Overview | **131**

show oam ethernet link-fault-management | **2822**

Example: Configuring Ethernet LFM with Loopback Support

In this example, LFM is configured between provider edge (PE) router and the customer edge (CE) router. The PE router can put the CE router in remote loopback mode. This allows the PE to have all the traffic sent to the CE router looped back for diagnostics purposes, as shown in Figure 16 on page 162.

Figure 16: Ethernet LFM with Loopback Support

To configure LFM between a PE router and a CE router:

1. Configure LFM loopback on the PE router:

```
[edit]
interfaces ge-1/0/0 {
    unit 0 {
        family inet {
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/0/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                    remote-loopback;
                }
            }
        }
    }
}
```

2. Configure LFM loopback on the CE router:

```
[edit]
```

```
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
}
```

NOTE: If the **negotiation options allow-remote-loopback** statement on the CE router is deleted before removing the CE router from remote loopback mode, traffic flow between the PE router and CE router is affected. Hence, delete the **remote-loopback** statement on the PE router before deleting the **negotiation-options allow-remote-loopback** statement on the CE router.

SEE ALSO

Example: Configuring Ethernet LFM Between Provider Edge and Customer Edge | **143**

Example: Configuring Ethernet LFM for CCC | **145**

Example: Configuring Ethernet LFM for Aggregated Ethernet | **146**

Release History Table

Release	Description
17.3R1	Starting in Junos OS Release 17.3R1, the Ethernet link fault management daemon (lfmd) runs on the backup Routing Engine as well when graceful Routing Engine switchover (GRES) is configured.

RELATED DOCUMENTATION

Introduction to OAM Link Fault Management (LFM) | **131**

Configuring Link Fault Management | **136**

CHAPTER 5

Ethernet Service OAM (ITU-TY.1731) for Routers

IN THIS CHAPTER

- ITU-T Y.1731 Ethernet Service OAM Overview | 165
- Configuring Ethernet Frame Delay Measurement Sessions | 185
- Configuring Ethernet Frame Loss Measurement | 223
- Configuring an Iterator Profile | 257
- Configuring Ethernet Synthetic Loss Measurements | 272
- Ethernet Alarm Indication | 286
- Inline Transmission Mode | 300

ITU-T Y.1731 Ethernet Service OAM Overview

IN THIS SECTION

- Ethernet Frame Delay Measurements Overview | 166
- Ethernet Frame Loss Measurement Overview | 172
- Service-Level Agreement Measurement | 174
- On-Demand Mode for SLA Measurement | 175
- Proactive Mode for SLA Measurement | 176
- Ethernet Failure Notification Protocol Overview | 177
- Ethernet Synthetic Loss Measurement Overview | 178
- Scenarios for Configuration of ETH-SLM | 179
- Format of ETH-SLM Messages | 181
- Transmission of ETH-SLM Messages | 182

Use this topic to understand more about service OAM (ITU-TY.1731) and its two main components: fault management (monitoring, detection, and isolation) and performance monitoring (frame loss measurement, synthetic frame loss measurement, and frame delay measurement).

Ethernet Frame Delay Measurements Overview

IN THIS SECTION

- ITU-T Y.1731 Frame Delay Measurement Feature | **166**
- One-Way Ethernet Frame Delay Measurement | **168**
- Two-Way Ethernet Frame Delay Measurement | **169**
- Choosing Between One-Way and Two-Way ETH-DM | **171**
- Restrictions for Ethernet Frame Delay Measurement | **171**

ITU-T Y.1731 Frame Delay Measurement Feature

The IEEE 802.3-2005 standard for Ethernet Operations, Administration, and Maintenance (OAM) defines a set of link fault management mechanisms to detect and report link faults on a single point-to-point Ethernet LAN.

Junos OS supports key OAM standards that provide for automated end-to-end management and monitoring of Ethernet service by service providers:

- *IEEE Standard 802.1ag*, also known as “Connectivity Fault Management (CFM).”
- *ITU-T Recommendation Y.1731*, which uses different terminology than IEEE 802.1ag and defines Ethernet service OAM features for fault monitoring, diagnostics, and performance monitoring.

These capabilities allow operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are tailored to the specific needs of their customers.

ACX Series routers support proactive and on-demand modes.

NOTE: ACX5048 and ACX5096 routers supports only software-based time stamping for delay measurement.

Ethernet CFM

The IEEE 802.1ag standard for connectivity fault management (CFM) defines mechanisms to provide for end-to-end Ethernet service assurance over any path, whether a single link or multiple links spanning networks composed of multiple LANs.

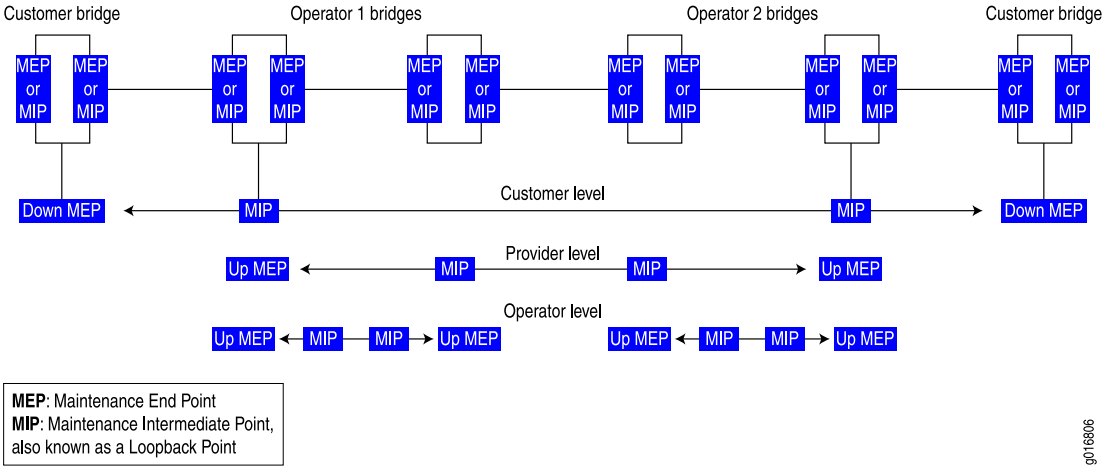
For Ethernet interfaces on M320, MX Series, and T Series routers, Junos OS supports the following key elements of the Ethernet CFM standard:

- Fault monitoring using the IEEE 802.1ag Ethernet OAM Continuity Check protocol
- Path discovery and fault verification using the IEEE 802.1ag Ethernet OAM Linktrace protocol
- Fault isolation using the IEEE 802.1ag Ethernet OAM Loopback protocol

In a CFM environment, network entities such as network operators, service providers, and customers may be part of different administrative domains. Each administrative domain is mapped into one maintenance domain. Maintenance domains are configured with different level values to keep them separate. Each domain provides enough information for the entities to perform their own management and end-to-end monitoring, and still avoid security breaches.

Figure 17 on page 167 shows the relationships among the customer, provider, and operator Ethernet bridges, maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs).

Figure 17: Relationship of MEPs, MIPs, and Maintenance Domain Levels



NOTE: On ACX Series routers, the maintenance intermediate points (MIP) is supported only on the ACX5048 and ACX5096 routers.

Ethernet Frame Delay Measurement

Two key objectives of OAM functionality are to measure quality-of-service attributes such as frame delay and frame delay variation (also known as “frame jitter”). Such measurements can enable you to identify network problems before customers are impacted by network defects.

Junos OS supports Ethernet frame delay measurement between MEPs configured on Ethernet physical or logical interfaces on MX Series routers. Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor SLAs. Ethernet frame delay measurement also collects other useful information, such as worst and best case delays, average delay, and average delay variation. The Junos OS implementation of Ethernet frame delay measurement (ETH-DM) is fully compliant with the ITU-T Recommendation Y.1731, *OAM Functions and Mechanisms for Ethernet-based Networks*. The recommendation defines OAM mechanisms for operating and maintaining the network at the Ethernet service layer, which is called the "ETH layer" in ITU-T terminology.

MX Series routers with modular port concentrators (MPCs) and 10-Gigabit Ethernet MPCs with SFP+ support ITU-T Y.1731 functionality on VPLS for frame-delay and delay-variation.

> **NOTE:** MX Series Virtual Chassis does not support Ethernet frame delay measurement (DM).

One-Way Ethernet Frame Delay Measurement

In one-way ETH-DM mode, a series of frame delay and frame delay variation values are calculated based on the time elapsed between the time a measurement frame is sent from the initiator MEP at one router and the time when the frame is received at the receiver MEP at the other router.

> **NOTE:** ACX Series routers do not support one-way Ethernet frame delay measurement.

1DM Transmission

When you start a one-way frame delay measurement, the router sends 1DM frames—frames that carry the protocol data unit (PDU) for a one-way delay measurement—from the initiator MEP to the receiver MEP at the rate and for the number of frames you specify. The router marks each 1DM frame as drop-ineligible and inserts a timestamp of the transmission time into the frame.

1DM Reception

When an MEP receives a 1DM frame, the router that contains the receiver MEP measures the one-way delay for that frame (the difference between the time the frame was received and the timestamp contained in the frame itself) and the delay variation (the difference between the current and previous delay values).

One-Way ETH-DM Statistics

The router that contains the receiver MEP stores each set of one-way delay statistics in the ETH-DM database. The ETH-DM database collects up to 100 sets of statistics for any given CFM session (pair of peer MEPs). You can access these statistics at any time by displaying the ETH-DM database contents.

One-Way ETH-DM Frame Counts

Each router counts the number of one-way ETH-DM frames sent and received:

- For an initiator MEP, the router counts the number of 1DM frames sent.
- For a receiver MEP, the router counts the number of valid 1DM frames received and the number of invalid 1DM frames received.

Each router stores ETH-DM frame counts in the CFM database. The CFM database stores CFM session statistics and, for interfaces that support ETH-DM, any ETH-DM frame counts. You can access the frame counts at any time by displaying CFM database information for Ethernet interfaces assigned to MEPs or for MEPs in CFM sessions.

Synchronization of System Clocks

The accuracy of one-way delay calculations depends on close synchronization of the system clocks at the initiator MEP and receiver MEP.

The accuracy of one-way delay variation is not dependent on system clock synchronization. Because delay variation is simply the difference between consecutive one-way delay values, the out-of-phase period is eliminated from the frame jitter values.

> **NOTE:** For a given one-way Ethernet frame delay measurement, frame delay and frame delay variation values are available only on the router that contains the receiver MEP.

Two-Way Ethernet Frame Delay Measurement

In two-way ETH-DM mode, frame delay and frame delay variation values are based on the time difference between when the initiator MEP transmits a request frame and receives a reply frame from the responder MEP, subtracting the time elapsed at the responder MEP.

DMM Transmission

When you start a two-way frame delay measurement, the router sends delay measurement message (DMM) frames— frames that carry the PDU for a two-way ETH-DM request—from the initiator MEP to the responder MEP at the rate and for the number of frames you specify. The router marks each DMM frame as drop-ineligible and inserts a timestamp of the transmission time into the frame.

DMR Transmission

When an MEP receives a DMM frame, the responder MEP responds with a delay measurement reply (DMR) frame, which carries ETH-DM reply information and a copy of the timestamp contained in the DMM frame.

DMR Reception

When an MEP receives a valid DMR, the router that contains the MEP measures the two-way delay for that frame based on the following sequence of timestamps:

1. TI_{TxDMM}
2. TR_{RxDMM}
3. TR_{TxDMR}
4. TI_{RxDMR}

A two-way frame delay is calculated as follows:

$$[TI_{RxDMR} - TI_{TxDMM}] - [TR_{TxDMR} - TR_{RxDMM}]$$

The calculation show that frame delay is the difference between the time at which the initiator MEP sends a DMM frame and the time at which the initiator MEP receives the associated DMR frame from the responder MEP, minus the time elapsed at the responder MEP.

The delay variation is the difference between the current and previous delay values.

Two-Way ETH-DM Statistics

The router that contains the initiator MEP stores each set of two-way delay statistics in the ETH-DM database. The ETH-DM database collects up to 100 sets of statistics for any given CFM session (pair of peer MEPs). You can access these statistics at any time by displaying the ETH-DM database contents.

Two-Way ETH-DM Frame Counts

Each router counts the number of two-way ETH-DM frames sent and received:

- For an initiator MEP, the router counts the number DMM frames transmitted, the number of valid DMR frames received, and the number of invalid DMR frames received.
- For a responder MEP, the router counts the number of DMR frames sent.

Each router stores ETH-DM frame counts in the CFM database. The CFM database stores CFM session statistics and, for interfaces that support ETH-DM, any ETH-DM frame counts. You can access the frame counts at any time by displaying CFM database information for Ethernet interfaces assigned to MEPs or for MEPs in CFM sessions.

NOTE: For a given two-way Ethernet frame delay measurement, frame delay and frame delay variation values are available only at the router that contains the initiator MEP.

Choosing Between One-Way and Two-Way ETH-DM

One-way frame delay measurement requires that the system clocks at the initiator MEP and receiver MEP are closely synchronized. Two-way frame delay measurement does not require synchronization of the two systems. If it is not practical for the clocks to be synchronized, two-way frame delay measurements are more accurate.

When two systems are physically close to each other, their one-way delay values are very high compared to their two-way delay values. One-way delay measurement requires that the timing for the two systems be synchronized at a very granular level, and MX Series routers currently do not support this granular synchronization.

Restrictions for Ethernet Frame Delay Measurement

The following restrictions apply to the Ethernet frame delay measurement feature:

- The ETH-DM feature is not supported on label-switched interface (LSI) pseudowires.

  The ETH-DM feature is supported on aggregated Ethernet interfaces.

- Hardware-assisted timestamping for ETH-DM frames in the reception path is only supported for MEP interfaces on Enhanced DPCs and Enhanced Queuing DPCs in MX Series routers. For information about hardware-assisted timestamping, see "Guidelines for Configuring Routers to Support an ETH-DM Session" on page 186 and "Enabling the Hardware-Assisted Timestamping Option" on page 198.

- Ethernet frame delay measurements can be triggered only when the distributed periodic packet management daemon (**ppm**) is enabled. For more information about this limitation, see "Guidelines for Configuring Routers to Support an ETH-DM Session" on page 186 and "Ensuring That Distributed ppm Is Not Disabled" on page 195.

- You can monitor only one session at a time to the same remote MEP or MAC address. For more information about starting an ETH-DM session, see "Starting an ETH-DM Session" on page 201.

- ETH-DM statistics are collected at only one of the two peer routers in the ETH-DM session. For a one-way ETH-DM session, you can display frame ETH-DM statistics at the receiver MEP only, using ETH-DM-specific **show** commands. For a two-way ETH-DM session, you can display frame delay statistics at the initiator MEP only, using the same ETH-DM-specific **show** commands. For more information, see "Managing ETH-DM Statistics and ETH-DM Frame Counts" on page 219.

- ETH-DM frame counts are collected at both MEPs and are stored in the respective CFM databases.

- If graceful Routing Engine switchover (GRES) occurs, any collected ETH-DM statistics are lost, and ETH-DM frame counts are reset to zeroes. Therefore, the collection of ETH-DM statistics and ETH-DM frame counters has to be restarted, after the switchover is complete. GRES enables a router with dual Routing Engines to switch from a master Routing Engine to a backup Routing Engine without interruption to packet forwarding. For more information, see the *High Availability User Guide*.

- Accuracy of frame delay statistics is compromised when the system is changing (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

SEE ALSO

Ethernet Alarm Indication | 286
Inline Transmission Mode | 300

Ethernet Frame Loss Measurement Overview

The key objectives of the OAM functionality are to measure quality-of-service attributes such as frame delay, frame delay variation (also known as “frame jitter”), and frame loss. Such measurements enable you to identify network problems before customers are impacted by network defects. For more information about Ethernet frame delay measurement, see “Ethernet Frame Delay Measurements Overview” on page 166.

Junos OS supports Ethernet frame loss measurement (ETH-LM) between maintenance association end points (MEPs) configured on Ethernet physical or logical interfaces on MX Series routers and is presently supported only for VPWS service. ETH-LM is used by operators to collect counter values applicable for ingress and egress service frames. These counters maintain a count of transmitted and received data frames between a pair of MEPs. Ethernet frame loss measurement is performed by sending frames with ETH-LM information to a peer MEP and similarly receiving frames with ETH-LM information from the peer MEP. This type of frame loss measurement is also known as single-ended Ethernet loss measurement.

NOTE: MX Series Virtual Chassis does not support Ethernet frame loss measurement (ETH-LM).

ETH-LM supports the following frame loss measurements:

- Near-end frame loss measurement—Measurement of frame loss associated with ingress data frames.
- Far-end frame loss measurement—Measurement of frame loss associated with egress data frames.

NOTE: The proactive and dual-ended loss measurement functionality of ITU-T Y1731 is not supported on the ACX Series routers.

The ETH-LM feature is supported on aggregated Ethernet interfaces.

NOTE: Starting Junos OS Release 16.1, the Ethernet loss measurement (ETH-LM) results are inaccurate when connectivity fault management (CFM) and performance monitoring (PM) PDUs received locally at a maintenance endpoint (MEP) as classified as belonging to the yellow class or a packet loss priority (PLP) of medium-high. This problem of incorrect results is specific to Ethernet loss measurement for CFM sessions of down MEPs. The Ethernet loss measurement statistics are inaccurate in the following scenarios:

- Ethernet loss measurement is working on a CFM session for a MEP in down state
- CFM PDUs received on the logical interface of the down MEP are classified by the classifier as yellow or medium-high PLP
- A packet is identified as yellow when the input classifier marks the PLP as medium-high.

The problem of discrepancies with Ethernet loss measurement results is not observed when you configure Ethernet loss measurement in colorless mode. To avoid this problem of inaccurate loss measurement results, provision all local CFM PDUs as green or with the PLP as high.

NOTE: Starting with Junos OS Release 16.1, performance monitoring for connectivity fault management (by including the **performance-monitoring** statement and its substatements at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level) is not supported when the network-to-network (NNI) or egress interface is an aggregated Ethernet interface with member links on DPCs.

SEE ALSO

Managing Continuity Measurement Statistics | **216**

Example: Measuring Ethernet Frame Loss for Single-Tagged LMM/LMR PDUs | **226**

Example: Measuring Ethernet Frame Loss for Dual-Tagged LMM/LMR PDUs | **242**

Service-Level Agreement Measurement

Service-level agreement (SLA) measurement is the process of monitoring the bandwidth, delay, delay variation (jitter), continuity, and availability of a service (E-Line or E-LAN). It enables you to identify network problems before customers are impacted by network defects.

> **NOTE:**
> The Ethernet VPN services can be classified into:
>
> - Peer-to-peer-services (E-Line services)—The E-Line services are offered using MPLS-based Layer 2 VPN virtual private wire service (VPWS).
> - Multipoint-to-multipoint services (E-LAN services)—The E-LAN services are offered using MPLS-based virtual private LAN service (VPLS).
>
> For more information, see the *Junos VPNs Configuration Guide*.

In Junos OS, SLA measurements are classified into:

- On-demand mode—In on-demand mode, the measurements are triggered through the CLI. For more information, see "On-Demand Mode for SLA Measurement" on page 175.
- Proactive mode—In proactive mode, the measurements are triggered by an iterator application. For more information, see "Proactive Mode for SLA Measurement" on page 176.

For more information about frame delay measurement, see "Ethernet Frame Delay Measurements Overview" on page 166. Note that Ethernet frame delay measurement and Ethernet frame loss measurement are not supported on the **ae** interface.

SEE ALSO

Ethernet Alarm Indication | **286**

Inline Transmission Mode | **300**

On-Demand Mode for SLA Measurement

In on-demand mode, the measurements are triggered by the user through the CLI.

When the user triggers the delay measurement through the CLI, the delay measurement request that is generated is as per the frame formats specified by the ITU-T Y.1731 standard. For two-way delay measurement, the server-side processing can be delegated to the Packet Forwarding Engine to prevent overloading on the Routing Engine. For more information, see "Configuring Routers to Support an ETH-DM Session" on page 194. When the server-side processing is delegated to the Packet Forwarding Engine, the delay measurement message (DMM) frame **receive** counters and delay measurement reply (DMR) frame **transmit** counters are not displayed by the **show** command.

When the user triggers the loss measurement through the CLI, the router sends the packets in standard format along with the loss measurement TLV. By default, the **session-id-tlv** argument is included in the packet to allow concurrent loss measurement sessions from same local MEP. You can also disable the session ID TLV by using the **no-session-id-tlv** argument.

Single-ended ETH-LM is used for on-demand operation, administration, and maintenance purposes. An MEP sends frames with ETH-LM request information to its peer MEP and receives frames with ETH-LM reply information from its peer MEP to carry out loss measurements. The protocol data unit (PDU) used for a single-ended ETH-LM request is referred to as a loss measurement message (LMM) and the PDU used for a single-ended ETH-LM reply is referred to as a loss measurement reply (LMR).

SEE ALSO

Configuring Ethernet Frame Loss Measurement | 223

Configuring an Iterator Profile | 257

Configuring Ethernet Synthetic Loss Measurements | 272

Proactive Mode for SLA Measurement

In proactive mode, SLA measurements are triggered by an iterator application. An iterator is designed to periodically transmit SLA measurement packets in form of ITU-Y.1731-compliant frames for two-way delay measurement or loss measurement on MX Series routers. This mode differs from on-demand SLA measurement, which is user initiated. The iterator sends periodic delay or loss measurement request packets for each of the connections registered to it. Iterators make sure that measurement cycles do not occur at the same time for the same connection to avoid CPU overload. Junos OS supports proactive mode for VPWS. For an iterator to form a remote adjacency and to become functionally operational, the continuity check message (CCM) must be active between the local and remote MEP configurations of the connectivity fault management (CFM). Any change in the iterator adjacency parameters resets the existing iterator statistics and restarts the iterator. Here, the term adjacency refers to a pairing of two endpoints (either connected directly or virtually) with relevant information for mutual understanding, which is used for subsequent processing. For example, the iterator adjacency refers to the iterator association between the two endpoints of the MEPs.

For every DPC or MPC, only 30 iterator instances for a cycle time value of 10 milliseconds (ms) are supported. In Junos OS, 255 iterator profile configurations and 2000 remote MEP associations are supported.

Iterators with cycle time value less than 100 ms are supported only for infinite iterators, whereas the iterators with cycle time value greater than 100 ms are supported for both finite and infinite iterators. Infinite iterators are iterators that run infinitely until the iterator is disabled or deactivated manually.

> **NOTE:** ACX5048 and ACX5096 routers supports iterator cycle time of only 1 second and above.

A VPWS service configured on a router is monitored for SLA measurements by registering the connection (here, the connection is a pair of remote and local MEPs) on an iterator and then initiating periodic SLA measurement frame transmission on those connections. The end-to-end service is identified through a maintenance association end point (MEP) configured at both ends.

For two-way delay measurement and loss measurement, an iterator sends a request message for the connection in the list (if any) and then sends a request message for the connection that was polled in the former iteration cycle. The back-to-back request messages for the SLA measurement frames and their responses help in computing delay variation and loss measurement.

The Y.1731 frame transmission for a service attached to an iterator continues endlessly unless intervened and stopped by an operator or until the iteration-count condition is met. To stop the iterator from sending out any more proactive SLA measurement frames, the operator must perform one of the following tasks:

- Enable the **deactivate sla-iterator-profile** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance association *ma-name* mep**

***mep-id* remote-mep *mep-id*]** hierarchy level. For more information, see "Verifying the Configuration of an Iterator Profile" on page 261.

- Provision a **disable** statement under the corresponding iterator profile at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles *profile-name*]** hierarchy level. For more information, see "Configuring an Iterator Profile" on page 258.

Ethernet Delay Measurements and Loss Measurement by Proactive Mode

In two-way delay measurement, the delay measurement message (DMM) frame is triggered through an iterator application. The DMM frame carries an iterator type, length, and value (TLV) in addition to the fields described in standard frame format and the server copies the iterator TLV from the DMM frame to the delay measurement reply (DMR) frame.

In one-way delay variation computation using the two-way delay measurement method, the delay variation computation is based on the timestamps that are present in the DMR frame (and not the 1DM frame). Therefore, there is no need for client-side and server-side clocks to be in sync. Assuming that the difference in their clocks remains constant, the one-way delay variation results are expected to be fairly accurate. This method also eliminates the need to send separate 1DM frames just for the one-way delay variation measurement purpose.

In proactive mode for loss measurement, the router sends packets in standard format along with loss measurement TLV and iterator TLV.

SEE ALSO

Configuring an Iterator Profile | 258

Configuring a Remote MEP with an Iterator Profile | 270

Verifying the Configuration of an Iterator Profile | 261

Managing Iterator Statistics | 264

Ethernet Failure Notification Protocol Overview

The Failure Notification Protocol (FNP) is a failure notification mechanism that detects failures in Point-to-Point Ethernet transport networks on MX Series routers. If a node link fails, FNP detects the failure and sends out FNP messages to the adjacent nodes that a circuit is down. Upon receiving the FNP message, nodes can redirect traffic to the protection circuit.

NOTE: FNP is supported on E-Line services only.

An E-Line service provides a secure Point-to-Point Ethernet connectivity between two user network interfaces (UNIs). E-Line services are a protected service and each service has a working circuit and protection circuit. CFM is used to monitor the working and protect paths. CCM intervals result in failover time in hundreds of milliseconds or a few seconds. FNP provides service circuit failure detection and propagation in less than 50ms and provide 50ms failover for E-Line services.

The MX router acts as a PE node and handles the FNP messages received on the management VLAN and the FNP messages received on both the Ethernet interfaces and PWs created for the management VPLS. MX-series routers do not initiate FNP messages and responds only to FNP messages generated by devices in the Ethernet Access network. FNP can be enabled only on logical interfaces that are part of a VPLS routing instance, and no physical interfaces in that VPLS routing instance should have CCM configured. FNP can be enabled only on one logical interface per physical interface.

All E-Line services are configured as layer 2 circuits with edge protection. A VLAN associated with the working circuit or protection circuit must map to a logical interface. No trunk port or access port is supported in the ring link for VLANs used by E-LINE services. FNP does not control the logical interface associated with protection circuit. Only E-Line service whose termination point is not in an MX node is controlled by FNP.

FNP supports graceful restart and the Graceful Routing Engine switchover (GRES) features.

SEE ALSO

Configuring the Failure Notification Protocol

show oam ethernet fnp interface | **2804**

show oam ethernet fnp status | **2808**

show oam ethernet fnp messages | **2806**

connectivity-fault-management

IEEE 802.1ag OAM Connectivity Fault Management Overview | **24**

Ethernet Synthetic Loss Measurement Overview

Ethernet synthetic loss measurement (ETH-SLM) is an application that enables the calculation of frame loss by using synthetic frames instead of data traffic. This mechanism can be considered as a statistical sample to approximate the frame loss ratio of data traffic. Each maintenance association end point (MEP) performs frame loss measurements, which contribute to unavailable time.

A near-end frame loss specifies frame loss associated with ingress data frames and a far-end frame loss specifies frame loss associated with egress data frames. Both near-end and far-end frame loss measurements contribute to near-end severely errored seconds and far-end severely errored seconds that are used in combination to determine unavailable time. ETH-SLM is performed using synthetic loss message (SLM) and synthetic loss reply (SLR) frames. ETH-SLM facilitates each MEP to perform near-end and far-end

synthetic frame loss measurements by using synthetic frames because a bidirectional service is defined as unavailable if either of the two directions is determined to be unavailable.

There are the two types of frame loss measurement, defined by the ITU-T Y.1731 standards, ETH-LM and ETH-SLM. Junos OS supports only single-ended ETH-SLM. In single-ended ETH-SLM, each MEP sends frames with the ETH-SLM request information to its peer MEP and receives frames with ETH-SLM reply information from its peer MEP to perform synthetic loss measurements. Single-ended ETH-SLM is used for proactive or on-demand OAM to perform synthetic loss measurements applicable to point-to-point Ethernet connection. This method allows a MEP to initiate and report far-end and near-end loss measurements associated with a pair of MEPs that are part of the same maintenance entity group (MEG).

NOTE: MX Series Virtual Chassis does not support Ethernet synthetic loss measurement (ETH-SLM).

Single-ended ETH-SLM is used to perform on-demand or proactive tests by initiating a finite amount of ETH-SLM frames to one or multiple MEP peers and receiving the ETH-SLM reply from the peers. The ETH-SLM frames contain the ETH-SLM information that is used to measure and report both near-end and far-end synthetic loss measurements. Service-level agreement (SLA) measurement is the process of monitoring the bandwidth, delay, delay variation (jitter), continuity, and availability of a service. It enables you to identify network problems before customers are impacted by network defects. In proactive mode, SLA measurements are triggered by an iterator application. An iterator is designed to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for synthetic frame loss measurement . This mode differs from on-demand SLA measurement, which is user initiated. In on-demand mode, the measurements are triggered by the user through the CLI. When the user triggers the ETH-SLM through the CLI, the SLM request that is generated is as per the frame formats specified by the ITU-T Y.1731 standard.

NOTE: ACX5048 and ACX5096 routers support ETH-SLM for Layer 2 services.

SEE ALSO

Troubleshooting Failures with ETH-SLM | 285

Scenarios for Configuration of ETH-SLM

ETH-SLM measures near-end and far-end frame loss between two MEPs that are part of the same MEG level. You can configure ETH-SLM to measure synthetic loss for both upward-facing or upstream MEP

and downward-facing or downstream MEP. This section describes the following scenarios for the operation of ETH-SLM:

Upstream MEP in MPLS Tunnels

Consider a scenario in which a MEP is configured between the user network interfaces (UNIs) of two MX Series routers, MX1 and MX2, in the upstream direction. MX1 and MX2 are connected over an MPLS core network. ETH-SLM measurements are performed between the upstream MEP in the path linking the two routers. Both MX1 and MX2 can initiate on-demand or proactive ETH-SLM, which can measure both far-end and near-end loss at MX1 and MX2, respectively. The two UNIs are connected using MPLS-based Layer 2 VPN virtual private wire service (VPWS).

Downstream MEP in Ethernet Networks

Consider a scenario in which a MEP is configured between two MX Series routers, MX1 and MX2, on the Ethernet interfaces in the downstream direction. MX1 and MX2 are connected in an Ethernet topology and downstream MEP is configured toward the Ethernet network. ETH-SLM measurements are performed between the downstream MEP in the path linking the two routers. ETH-SLM can be measured in the path between these two routers.

Consider another scenario in which a MEP is configured in the downstream direction and service protection for a VPWS over MPLS is enabled by specifying a working path or protect path on the MEP. Service protection provides end-to-end connection protection of the working path in the event of a failure. To configure service protection, you must create two separate transport paths—a working path and a protect path. You can specify the working path and protect path by creating two maintenance associations. To associate the maintenance association with a path, you must configure the MEP interface in the maintenance association and specify the path as working or protect.

In a sample topology, an MX Series router, MX1, is connected to two other MX Series routers, MX2 and MX3, over an MPLS core. The connectivity fault management (CFM) session between MX1 and MX2 is the working path on the MEP and the CFM session between MX1 and MX3 is the protect path on the MEP. MX2 and MX3 are, in turn, connected on Ethernet interfaces to MX4 in the access network. Downstream MEP is configured between MX1 and MX4 that passes through MX2 (working CFM session) and also between MX1 and MX4 that passes through MX3 (protected CFM session). ETH-SLM is performed between these downstream MEPs. In both the downstream MEPs, the configuration is performed on MX1 and MX4 UNIs, similar to upstream MEP.

SEE ALSO

Troubleshooting Failures with ETH-SLM | 285

Format of ETH-SLM Messages

Synthetic loss messages (SLMs) support single-ended Ethernet synthetic loss measurement (ETH-SLM) requests. This topic contains the following sections that describe the formats of the SLM protocol data units (PDUs), SLR PDUs, and the data iterator type length value (TLV).

SLM PDU Format

The SLM PDU format is used by a MEP to transmit SLM information. The following components are contained in SLM PDUs:

- Source MEP ID—Source MEP ID is a 2-octet field where the last 13 least significant bits are used to identify the MEP transmitting the SLM frame. MEP ID is unique within the MEG.
- Test ID—Test ID is a 4-octet field set by the transmitting MEP and is used to identify a test when multiple tests run simultaneously between MEPs (including both concurrent on-demand and proactive tests).
- TxFCf—TxFCf is a 4-octet field that carries the number of SLM frames transmitted by the MEP toward its peer MEP.

The following are the fields in an SLM PDU:

- MEG Level—Configured maintenance domain level in the range 0–7.
- Version—0.
- OpCode—Identifies an OAM PDU type. For SLM, it is 55.
- Flags—Set to all zeros.
- TLV Offset—16.
- Source MEP ID—A 2-octet field used to identify the MEP transmitting the SLM frame. In this 2-octet field, the last 13 least significant bits are used to identify the MEP transmitting the SLM frame. MEP ID is unique within the MEG.
- RESV—Reserved fields are set to all zeros.
- Test ID—A 4-octet field set by the transmitting MEP and used to identify a test when multiple tests run simultaneously between MEPs (including both concurrent on-demand and proactive tests).
- TxFCf—A 4-octet field that carries the number of SLM frames transmitted by the MEP toward its peer MEP.
- Optional TLV—A data TLV may be included in any SLM transmitted. For the purpose of ETH-SLM, the value part of data TLV is unspecified.
- End TLV—All zeros octet value.

SLR PDU Format

The synthetic loss reply (SLR) PDU format is used by a MEP to transmit SLR information. The following are the fields in an SLR PDU:

- MEG Level—A 3-bit field the value of which is copied from the last received SLM PDU.
- Version—A 5-bit field the value of which is copied from the last received SLM PDU.
- OpCode—Identifies an OAM PDU type. For SLR, it is set as 54.
- Flags—A 1-octet field copied from the SLM PDU.
- TLV Offset—A 1-octet field copied from the SLM PDU.
- Source MEP ID—A 2-octet field copied from the SLM PDU.
- Responder MEP ID—A 2-octet field used to identify the MEP transmitting the SLR frame.
- Test ID—A 4-octet field copied from the SLM PDU.
- TxFCf—A 4-octet field copied from the SLM PDU.
- TxFCb—A 4 octet field. This value represents the number of SLR frames transmitted for this test ID.
- Optional TLV—The value is copied from the SLM PDU, if present.
- End TLV—A 1-octet field copied from the SLM PDU.

Data Iterator TLV Format

The data iterator TLV specifies the data TLV portion of the Y.1731 data frame. The MEP uses a data TLV when the MEP is configured to measure delay and delay variation for different frame sizes. The following are the fields in a data TLV:

- Type—Identifies the TLV type; value for this TLV type is Data (3).
- Length—Identifies the size, in octets, of the Value field containing the data pattern. The maximum value of the Length field is 1440.
- Data pattern—An *n*-octet (*n* denotes length) arbitrary bit pattern. The receiver ignores it.

SEE ALSO

Troubleshooting Failures with ETH-SLM | **285**

Transmission of ETH-SLM Messages

The ETH-SLM functionality can process multiple synthetic loss message (SLM) requests simultaneously between a pair of MEPs. The session can be a proactive or an on-demand SLM session. Each SLM request is identified uniquely by a test ID.

A MEP can send SLM requests or respond to SLM requests. A response to an SLM request is called a synthetic loss reply (SLR). After a MEP determines an SLM request by using the test ID, the MEP calculates the far-end and near-end frame loss on the basis of the information in the SLM message or the SLM protocol data unit (PDU).

A MEP maintains the following local counters for each test ID and for each peer MEP being monitored in a maintenance entity for which loss measurements are to be performed:

- TxFCl—Number of synthetic frames transmitted toward the peer MEP for a test ID. A source MEP increments this number for successive transmission of synthetic frames with ETH-SLM request information while a destination or receiving MEP increments this value for successive transmission of synthetic frames with the SLR information.
- RxFCl—Number of synthetic frames received from the peer MEP for a test ID. A source MEP increments this number for successive reception of synthetic frames with SLR information while a destination or receiving MEP increments it for successive reception of synthetic frames with ETH-SLM request information.

The following sections describe the phases of processing of SLM PDUs to determine synthetic frame loss:

Initiation and Transmission of SLM Requests

A MEP periodically transmits an SLM request with the OpCode field set as 55. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TxFCl is sent in the packet.

No synchronization is required of the test ID value between initiating and responding MEPs because the test ID is configured at the initiating MEP, and the responding MEP uses the test ID it receives from the initiating MEP. Because ETH-SLM is a sampling technique, it is less precise than counting the service frames. Also, the accuracy of measurement depends on the number of SLM frames used or the period for transmitting SLM frames.

Reception of SLMs and Transmission of SLRs

After the destination MEP receives a valid SLM frame from the source MEP, an SLR frame is generated and transmitted to the requesting or source MEP. The SLR frame is valid if the MEG level and the destination MAC address match the receiving MEP's MAC address. All the fields in the SLM PDUs are copied from the SLM request except for the following fields:

- The source MAC address is copied to the destination MAC address and the source address contains the MEP's MAC address.
- The value of the OpCode field is changed from SLM to SLR (54).
- The responder MEP ID is populated with the MEP's MEP ID.
- TxFCb is saved with the value of the local counter RxFCl at the time of SLR frame transmission.
- An SLR frame is generated every time an SLM frame is received; therefore, RxFCl in the responder is equal to the number of SLM frames received and also equal to the number of SLR frames sent. At the responder or receiving MEP, RxFCl equals TxFCl.

Reception of SLRs

After an SLM frame (with a given TxFCf value) is transmitted, a MEP expects to receive a corresponding SLR frame (carrying the same TxTCf value) within the timeout value from its peer MEP. SLR frames that are received after the timeout value (5 seconds) are discarded. With the information contained in SLR frames, a MEP determines the frame loss for the specified measurement period. The measurement period is a time interval during which the number of SLM frames transmitted is statistically adequate to make a measurement at a given accuracy. A MEP uses the following values to determine near-end and far-end frame loss during the measurement period:

- Last received SLR frame's TxFCf and TxFCb values and the local counter RxFCl value at the end of the measurement period. These values are represented as TxFCf[tc], TxFCb[tc], and RxFCl[tc], where tc is the end time of the measurement period.
- SLR frame's TxFCf and TxFCb values of the first received SLR frame after the test starts and local counter RxFCl at the beginning of the measurement period. These values are represented as TxFCf[tp], TxFCb[tp], and RxFCl[tp], where tp is the start time of the measurement period.

For each SLR packet that is received, the local RxFCl counter is incremented at the sending or source MEP.

Reception of SLRs

After an SLM frame (with a given TxFCf value) is transmitted, a MEP expects to receive a corresponding SLR frame (carrying the same TxTCf value) within the timeout value from its peer MEP. SLR frames that are received after the timeout value (5 seconds) are discarded. With the information contained in SLR frames, a MEP determines the frame loss for the specified measurement period. The measurement period is a time interval during which the number of SLM frames transmitted is statistically adequate to make a measurement at a given accuracy. A MEP uses the following values to determine near-end and far-end frame loss during the measurement period:

- Last received SLR frame's TxFCf and TxFCb values and the local counter RxFCl value at the end of the measurement period. These values are represented as TxFCf[tc], TxFCb[tc], and RxFCl[tc], where tc is the end time of the measurement period.
- SLR frame's TxFCf and TxFCb values of the first received SLR frame after the test starts and local counter RxFCl at the beginning of the measurement period. These values are represented as TxFCf[tp], TxFCb[tp], and RxFCl[tp], where tp is the start time of the measurement period.

For each SLR packet that is received, the local RxFCl counter is incremented at the sending or source MEP.

SEE ALSO

Troubleshooting Failures with ETH-SLM | 285

Release History Table

Release	Description
16.1	Starting Junos OS Release 16.1, the Ethernet loss measurement (ETH-LM) results are inaccurate when connectivity fault management (CFM) and performance monitoring (PM) PDUs received locally at a maintenance endpoint (MEP) as classified as belonging to the yellow class or a packet loss priority (PLP) of medium-high.
16.1	Starting with Junos OS Release 16.1, performance monitoring for connectivity fault management (by including the **performance-monitoring** statement and its substatements at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level) is not supported when the network-to-network (NNI) or egress interface is an aggregated Ethernet interface with member links on DPCs.

RELATED DOCUMENTATION

- Configuring Ethernet Frame Loss Measurement | **223**
- Configuring an Iterator Profile | **257**
- Configuring Ethernet Synthetic Loss Measurements | **272**

Configuring Ethernet Frame Delay Measurement Sessions

IN THIS SECTION

- Guidelines for Configuring Routers to Support an ETH-DM Session | **186**
- Guidelines for Starting an ETH-DM Session | **187**
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts | **189**
- Configuring Routers to Support an ETH-DM Session | **194**
- Triggering an Ethernet Frame Delay Measurements Session | **199**
- Starting an ETH-DM Session | **201**
- Example: Configuring One-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | **204**
- Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | **210**
- Managing Continuity Measurement Statistics | **216**
- Viewing Ethernet Frame Delay Measurements Statistics | **217**
- Managing ETH-DM Statistics and ETH-DM Frame Counts | **219**

Use this topic to understand how to configure Ethernet frame delay measurement sessions. You can start either a one-way Ethernet delay measurement session or a two-way Ethernet delay measurement session. Also, use this topic to view the delay measurement statistics and frame counts.

Guidelines for Configuring Routers to Support an ETH-DM Session

IN THIS SECTION

- Configuration Requirements for ETH-DM | **186**
- Configuration Options for ETH-DM | **187**

Keep the following guidelines in mind when configuring routers to support an Ethernet frame delay measurement (ETH-DM) session:

Configuration Requirements for ETH-DM

You can obtain ETH-DM information for a link that meets the following requirements:

- The measurements can be performed between peer maintenance association endpoints (MEPs) on two routers.
- The two MEPs must be configured on two Ethernet physical interfaces or on two Ethernet logical interfaces. For more information, see "Configuring a MEP to Generate and Respond to CFM Protocol Messages" on page 40.
- The two MEPs must be configured—on their respective routers—under the same maintenance association (MA) identifier. For more information, see "Creating a Maintenance Association" on page 37.
- On both routers, the MA must be associated with the same maintenance domain (MD) name. For more information, see "Creating a Maintenance Domain" on page 31.
- On both routers, periodic packet management (PPM) must be running on the Routing Engine and Packet Forwarding Engine, which is the default configuration. You can disable PPM on the Packet Forwarding Engine only. However, the Ethernet frame delay measurement feature requires that distributed PPM remain enabled on the Packet Forwarding Engine of both routers. For more information about **ppm**, see the *Junos OS Routing Protocols Library*.
- If the PPM process (**ppm**) is disabled on the Packet Forwarding Engine, you must re-enable it. Re-enabling distributed **ppm** entails restarting the **ethernet-connectivity-fault-management** process, which causes all connectivity fault management (CFM) sessions to re-establish. For more information about CFM sessions, see "Configuring Ethernet Local Management Interface" on page 55.

NOTE: The Ethernet frame delay measurement feature is supported only for MEPs configured on Ethernet physical or logical interfaces on DPCs in MX Series routers. The ETH-DM feature is not supported on aggregated Ethernet interfaces or LSI pseudowires.

Configuration Options for ETH-DM

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.

SEE ALSO

Ethernet Alarm Indication | 286
Inline Transmission Mode | 300

Guidelines for Starting an ETH-DM Session

IN THIS SECTION

- ETH-DM Session Prerequisites | 187
- ETH-DM Session Parameters | 188
- Restrictions for an ETH-DM Session | 189

Keep the following guidelines in mind when preparing to start an Ethernet frame delay measurement (ETH-DM) session:

ETH-DM Session Prerequisites

Before you can start an ETH-DM session, you must configure two MX Series routers to support ETH-DM by defining the two CFM-enabled physical or logical Ethernet interfaces on each router. This entails creating and configuring CFM maintenance domains, maintenance associations, and maintenance association end points on each router. For more information about enabling CFM on an Ethernet interface, see “Creating a Maintenance Domain” on page 31.

> **NOTE:** The Ethernet frame delay measurement feature is supported only for maintenance association end points configured on Ethernet physical or logical interfaces on DPCs in MX Series routers. The ETH-DM feature is not supported on aggregated Ethernet interfaces or LSI pseudowires.

For specific information about configuring routers to support ETH-DM, see"Guidelines for Configuring Routers to Support an ETH-DM Session" on page 186 and "Configuring Routers to Support an ETH-DM Session" on page 194.

ETH-DM Session Parameters

You can initiate a one-way or two-way ETH-DM session by entering the **monitor ethernet delay-measurement** operational command at a router that contains one end of the service for which you want to measure frame delay. The command options specify the ETH-DM session in terms of the CFM elements:

- The type of ETH-DM measurement (one-way or two-way) to be performed.
- The Ethernet service for which the ETH-DM measurement is to be performed:
  - CFM maintenance domain—Name of the existing maintenance domain (MD) for which you want to measure Ethernet frame delays. For more information, see "Creating a Maintenance Domain" on page 31.
  - CFM maintenance association—Name of an existing maintenance association (MA) within the maintenance domain. For more information, see "Creating a Maintenance Association" on page 37.
  - Remote CFM maintenance association end point—The unicast MAC address or the numeric identifier of the remote maintenance association end point (MEP)—the physical or logical interface on the remote router that resides in the specified MD and is named in the specified MA—with which to perform the ETH-DM session. For more information, see "Configuring a MEP to Generate and Respond to CFM Protocol Messages" on page 40.
- Optional specifications:
  - Count—You can specify the number of ETH-DM requests to send for this frame delay measurement session. The range is from 1 through 65,535 frames. The default value is 10 frames.

    NOTE: Although you can trigger frame delay collection for up to 65,535 ETH-DM requests at a time, a router stores only the last 100 frame delay statistics per CFM session (pair of peer MEPs).
  - Frame interval—You can specify the number of seconds to elapse between ETH-DM frame transmittals. The default value is 1 second.

For more detailed information about the parameters you can specify to start an ETH-DM session, see the **monitor ethernet delay-measurement** operational command description in the CLI Explorer.

Restrictions for an ETH-DM Session

The following restrictions apply to an ETH-DM session:

- You cannot run multiple simultaneous ETH-DM sessions with the same remote MEP or MAC address.
- For a given ETH-DM session, you can collect frame delay information for a maximum of 65,535 frames.
- For a given CFM session (pair of peer MEPs), the ETH-DM database stores a maximum of 100 statistics, with the older statistics being "aged out" as newer statistics are collected for that pair of MEPs.
  - For one-way delay measurements collected within the same CFM session, the 100 most recent ETH-DM statistics can be retrieved at any point of time at the router on which the receiver MEP is defined.
  - For two-way delay measurements collected within the same CFM session, the 100 most recent ETH-DM statistics can be retrieved at any point of time at the router on which the initiator MEP is defined.

  Depending on the number of frames exchanged in the individual ETH-DM sessions, the ETH-DM database can contain statistics collected through multiple ETH-DM sessions.
- If graceful Routing Engine switchover (GRES) occurs, any collected ETH-DM statistics are lost, and ETH-DM frame counts are reset to zeroes. GRES enables a router with dual Routing Engines to switch from a master Routing Engine to a backup Routing Engine without interruption to packet forwarding. For more information, see the *High Availability User Guide*.
- Accuracy of frame delay data is compromised when the system is changing (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

SEE ALSO

Using the monitor ethernet delay-measurement Command | **201**

monitor ethernet delay-measurement | **2657**

Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts

IN THIS SECTION

- ETH-DM Statistics | **190**
- ETH-DM Statistics Retrieval | **192**
- ETH-DM Frame Counts | **192**
- ETH-DM Frame Count Retrieval | **193**

ETH-DM Statistics

Ethernet frame delay statistics are the frame delay and frame delay variation values determined by the exchange of frames containing ETH-DM protocol data units (PDUs).

- For a one-way ETH-DM session, statistics are collected in an ETH-DM database at the router that contains the receiver MEP. For a detailed description of one-way Ethernet frame delay measurement, including the exchange of one-way delay PDU frames, see "Ethernet Frame Delay Measurements Overview" on page 166.
- For a two-way ETH-DM session, statistics are collected in an ETH-DM database at the router that contains the initiator MEP. For a detailed description of two-way Ethernet frame delay measurement, including the exchange of two-way delay PDU frames, see "Ethernet Frame Delay Measurements Overview" on page 166.

A CFM database stores CFM-related statistics and—for Ethernet interfaces that support ETH-DM—the 100 most recently collected ETH-DM statistics for that pair of MEPs. You can view ETH-DM statistics by using the **delay-statistics** or **mep-statistics** form of the **show oam ethernet connectivity-fault-management** command to display the CFM statistics for the MEP that collects the ETH-DM statistics you want to view.

Table 15 on page 190 describes the ETH-DM statistics calculated in an ETH-DM session.

Table 15: ETH-DM Statistics

Field Name	Field Description
One-way delay (µsec)†	For a one-way ETH-DM session, the frame delay, in microseconds, collected at the receiver MEP. To display frame delay statistics for a given one-way ETH-DM session, use the **delay-statistics** or **mep-statistics** form of the **show oam ethernet connectivity-fault-management** command at the receiver MEP for that session.
Two-way delay (µsec)	For a two-way ETH-DM session, the frame delay, in microseconds, collected at the initiator MEP. When you start a two-way frame delay measurement, the CLI output displays each DMR frame receipt timestamp and corresponding DMM frame delay and delay variation collected as the session progresses. To display frame delay statistics for a given two-way ETH-DM session, use the **delay-statistics** or **mep-statistics** form of the **show oam ethernet connectivity-fault-management** command at the initiator MEP for that session.

Table 15: ETH-DM Statistics *(continued)*

Field Name	Field Description
Average delay[†]	When you start a two-way frame delay measurement, the CLI output includes a runtime display of the average two-way frame delay among the statistics collected for the ETH-DM session only. When you display ETH-DM statistics using a **show** command, the **Average delay** field displays the average one-way and two- frame delays among all ETH-DM statistics collected at the CFM session level. For example, suppose you start two one-way ETH-DM sessions for 50 counts each, one after the other. If, after both measurement sessions complete, you use a **show** command to display 100 ETH-DM statistics for that CFM session, the **Average delay** field displays the average frame delay among all 100 statistics.
Average delay variation[†]	When you start a two-way frame delay measurement, the CLI output includes a runtime display of the average two-way frame delay variation among the statistics collected for the ETH-DM session only. When you display ETH-DM statistics using a **show** command, the **Average delay variation** field displays the average one-way and two- frame delay variations among all ETH-DM statistics collected at the CFM session level.
Best-case delay[†]	When you start a two-way frame delay measurement, the CLI output includes a runtime display of the lowest two-way frame delay value among the statistics collected for the ETH-DM session only. When you display ETH-DM statistics using a **show** command, the **Best case delay** field displays the lowest one-way and two-way frame delays among all ETH-DM statistics collected at the CFM session level.
Worst-case delay[†]	When you start a two-way frame delay measurement, the CLI output includes a runtime display of the highest two-way frame delay value among the statistics collected for the ETH-DM session only. When you display ETH-DM statistics using a **show** command, the **Worst case delay** field displays the highest one-way and two-way frame delays among all statistics collected at the CFM session level.

[†]When you start a one-way frame delay measurement, the CLI output displays **NA** (“not available”) for this field. One-way ETH-DM statistics are collected at the remote (receiver) MEP. Statistics for a given one-way ETH-DM session are available only by displaying CFM statistics for the receiver MEP.

ETH-DM Statistics Retrieval

At the receiver MEP for a one-way session, or at the initiator MEP for a two-way session, you can display all ETH-DM statistics collected at a CFM session level by using the following operational commands:

- **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain *md-name* maintenance-association *ma-name* <local-mep *mep-id*> <remote-mep *mep-id*> <count *count*>**
- **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain *md-name* maintenance-association *ma-name* <local-mep *mep-id*> <remote-mep *mep-id*> <count *count*>**

ETH-DM Frame Counts

The number of ETH-DM PDU frames exchanged in a ETH-DM session are stored in the CFM database on each router.

Table 16 on page 192 describes the ETH-DM frame counts collected in an ETH-DM session.

Table 16: ETH-DM Frame Counts

Field Name	Field Description
1DMs sent	Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. Stored in the CFM database of the MEP initiating a one-way frame delay measurement.
Valid 1DMs received	Number of valid 1DM frames received. Stored in the CFM database of the MEP receiving a one-way frame delay measurement.
Invalid 1DMs received	Number of invalid 1DM frames received. Stored in the CFM database of the MEP receiving a one-way frame delay measurement.
DMMs sent	Number of delay measurement message (DMM) PDU frames sent to the peer MEP in this session. Stored in the CFM database of the MEP initiating a two-way frame delay measurement.
DMRs sent	Number of delay measurement reply (DMR) frames sent (in response to a received DMM). Stored in the CFM database of the MEP responding to a two-way frame delay measurement.
Valid DMRs received	Number of valid DMR frames received. Stored in the CFM database of the MEP initiating a two-way frame delay measurement.
Invalid DMRs received	Number of invalid DMR frames received. Stored in the CFM database of the MEP initiating a two-way frame delay measurement.

ETH-DM Frame Count Retrieval

Each router counts the number of ETH-DM frames sent or received and stores the counts in a CFM database.

Frame Counts Stored in CFM Databases

You can display ETH-DM frame counts for MEPs assigned to specified Ethernet interfaces or for specified MEPs in CFM sessions by using the following operational commands:

- **show oam ethernet connectivity-fault-management interfaces** (**detail** | **extensive**)
- **show oam ethernet connectivity-fault-management mep-database maintenance-domain** ***md-name*** **maintenance-association** ***ma-name*** **<local-mep** ***mep-id*****> <remote-mep** ***mep-id*****>**

One-Way ETH-DM Frame Counts

For a one-way ETH-DM session, delay statistics are collected at the receiver MEP only, but frame counts are collected at both MEPs. As indicated in Table 16 on page 192, one-way ETH-DM frame counts are tallied from the perspective of each router in the session:

- At the initiator MEP, the router counts the number of 1DM frames sent.
- At the receiver MEP, the router counts the number of valid 1DM frames received and the number of invalid 1DM frames received.

You can also view one-way ETH-DM frame counts—for a receiver MEP—by using the **show oam ethernet connectivity-fault-management mep-statistics** command to display one-way statistics and frame counts together.

Two-Way ETH-DM Frame Counts

For a two-way ETH-DM session, delay statistics are collected at the initiator MEP only, but frame counts are collected at both MEPs. As indicated in Table 16 on page 192, two-way ETH-DM frame counts are tallied from the perspective of each router in the session:

- At the initiator MEP, the router counts the number of DMM frames sent, valid DMR frames received, and invalid DMR frames received.
- At the responder MEP, the router counts the number of DMR frames sent.

You can also view two-way ETH-DM frame counts—for an initiator MEP—by using the **show oam ethernet connectivity-fault-management mep-statistics** command to display two-way statistics and frame counts together.

SEE ALSO

clear oam ethernet connectivity-fault-management statistics | 2647 command

show oam ethernet connectivity-fault-management mep-statistics | 2764 command

show oam ethernet connectivity-fault-management delay-statistics | 2679 command

show oam ethernet connectivity-fault-management interfaces | 2727 (**detail** | **extensive**) command

show oam ethernet connectivity-fault-management mep-database | 2749 command

Configuring Routers to Support an ETH-DM Session

IN THIS SECTION

- Configuring MEP Interfaces | **194**
- Ensuring That Distributed ppm Is Not Disabled | **195**
- Enabling the Hardware-Assisted Timestamping Option | **198**
- Configuring the Server-Side Processing Option | **198**

Configuring MEP Interfaces

Before you can start an Ethernet frame delay measurement session across an Ethernet service, you must configure two MX Series routers to support ETH-DM.

To configure an Ethernet interface on a MX Series router to support ETH-DM:

1. On each router, configure two physical or logical Ethernet interfaces connected by a VLAN. The following configuration is typical for single-tagged logical interfaces:

```
[edit interfaces]
interface {
    ethernet-interface-name {
        vlan-tagging;
        unit logical-unit-number {
            vlan-id vlan-id; # Both interfaces on this VLAN
        }
    }
}
```

   Both interfaces will use the same VLAN ID.

2. On each router, attach peer MEPs to the two interfaces. The following configuration is typical:

```
[edit protocols]
oam {
```

```
ethernet {
    connectivity-fault-management {
        maintenance-domain md-name { # On both routers
            level number;
            maintenance-association ma-name { # On both routers
                continuity-check {
                    interval 100ms;
                    hold-interval 1;
                }
                mep mep-id { # Attach to VLAN interface
                    auto-discovery;
                    direction (up | down);
                    interface interface-name;
                    priority number;
                }
            }
        }
    }
}
```

Ensuring That Distributed ppm Is Not Disabled

By default, the router's period packet management process (**ppm**) runs sessions distributed to the Packet Forwarding Engine in addition to the Routing Engine. This process is responsible for periodic transmission of packets on behalf of its various client processes, such as Bidirectional Forwarding Detection (BFD), and it also receives packets on behalf of client processes.

In addition, **ppm** handles time-sensitive periodic processing and performs such processes as sending process-specific packets and gathering statistics. With **ppm** processes running distributed on both the Routing Engine and the Packet Forwarding Engine, you can run such processes as BFD on the Packet Forwarding Engine.

Distributed ppm Required for ETH-DM

Ethernet frame delay measurement requires that **ppm** remains distributed to the Packet Forwarding Engine. If **ppm** is not distributed to the Packet Forwarding Engines of both routers, ETH-DM PDU frame timestamps and ETH-DM statistics are not valid.

Before you start ETH-DM, you must verify that the following configuration statement is *NOT* present:

```
[edit]
```

```
routing-options {
    ppm {
        no-delegate-processing;
    }
}
```

If distributed **ppm** processing is disabled (as shown in the stanza above) on either router, you must re-enable it in order to use the ETH-DM feature.

Procedure to Ensure that Distributed ppm is Not Disabled

To ensure that distributed **ppm** is not disabled on a router:

1. Display the packet processing management (PPM) configuration to determine whether distributed **ppm** is disabled.

   - In the following example, distributed **ppm** is enabled on the router. In this case, you do not need to modify the router configuration:

     ```
     [edit]
     user@host# show routing-options
     ppm;
     ```

   - In the following example, distributed **ppm** is disabled on the router. In this case, you must proceed to Step 2 to modify the router configuration:

     ```
     [edit]
     user@host show routing-options
     ppm {
         no-delegate-processing;
     }
     ```

2. Modify the router configuration to re-enable distributed **ppm** and restart the Ethernet OAM Connectivity Fault Management process *ONLY IF* distributed **ppm** is disabled (as determined in the previous step).

   a. Before continuing, make any necessary preparations for the possible loss of connectivity on the router.

      Restarting the **ethernet-connectivity-fault-management** process has the following effect on your network:

      - All connectivity fault management (CFM) sessions re-establish.
      - All ETH-DM requests on the router terminate.
      - All ETH-DM statistics and frame counts reset to 0.

   b. Modify the router configuration to re-enable distributed **ppm**. For example:

      ```
      [edit]
      user@host# delete routing-options ppm no-delegate-processing
      ```

   c. Commit the updated router configuration. For example:

      ```
      [edit]
      user@host# commit and-quit
      commit complete
      exiting configuration mode
      ```

   d. To restart the Ethernet OAM Connectivity-Fault-Management process, enter the **restart ethernet-connectivity-fault-management <gracefully | immediately | soft>** operational mode command. For example:

      ```
      user@host> restart ethernet-connectivity-fault-management
      Connectivity fault management process started, pid 9893
      ```

Connectivity fault management (CFM) sessions operate in centralized mode over AE interfaces by default. Y.1731 performance monitoring (PM) is supported on centralized CFM sessions over AE interfaces. Also, distribution of CFM session over AE interfaces to line cards is supported from Junos OS Release 13.3. To enable the distribution of CFM sessions and to operate in centralized mode, include the **ppm delegate-processing** statement at the **[edit routing-options ppm]** hierarchy level. The mechanism that enables distribution of CFM sessions over AE interfaces provides the underlying infrastructure to support PM over AE interfaces. In addition, periodic packet management (PPM) handles time-sensitive periodic processing and performs such processes as sending process-specific packets and gathering statistics. With PPM processes running distributed on both the Routing Engine and the Packet Forwarding Engine, you can run performance monitoring processes on the Packet Forwarding Engine.

SEE ALSO

Periodic Packet Management

Understanding Periodic Packet Management on MX Series Routers

Enabling the Hardware-Assisted Timestamping Option

By default, Ethernet frame delay measurement uses software for timestamping transmitted and received ETH-DM frames. For Ethernet interfaces, you can optionally use hardware timing to assist in the timestamping of received ETH-DM frames to increase the accuracy of delay measurements.

Enabling hardware-assisted timestamping of received frames can increase the accuracy of ETH-DM calculations when the DPC is loaded with heavy traffic in the receive direction.

To enable Ethernet frame delay measurement hardware assistance on the reception path, include the **hardware-assisted-timestamping** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            performance-monitoring {
                hardware-assisted-timestamping;
            }
        }
    }
}
```

SEE ALSO

hardware-assisted-timestamping | **1796**

Configuring the Server-Side Processing Option

You can delegate the server-side processing (for both two-way delay measurement and loss measurement) to the Packet Forwarding Engine to prevent overloading on the Routing Engine. By default, the server-side processing is done by the Routing Engine.

To configure the server-side processing option:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure the server-side processing option.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set delegate-server-processing
```

3. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# show
performance-monitoring {
    delegate-server-processing;
}
```

SEE ALSO

delegate-server-processing | 1784

SEE ALSO

Understanding Periodic Packet Management on MX Series Routers

Inline Transmission Mode | 300

Triggering an Ethernet Frame Delay Measurements Session

Before Ethernet frame delay measurement statistics can be displayed, they must be collected. To trigger Ethernet frame delay measurement, use the **monitor ethernet delay-measurement (one-way | two-way) (*remote-mac-address*) maintenance-domain *name* maintenance-association *ma-id* [count *count*] [wait *time*]** operational command.

The fields for this command are described in Table 17 on page 199.

Table 17: Monitor Ethernet Delay Command Parameters

Parameter	Parameter Range	Description
one-way or **two-way** or	NA	Perform a one-way or two-way (round-trip) delay measurement.

Table 17: Monitor Ethernet Delay Command Parameters *(continued)*

Parameter	Parameter Range	Description
remote-mac-address	Unicast MAC address	Send delay measurement frames to the destination unicast MAC address (use the format xx:xx:xx:xx:xx:xx). Multicast MAC addresses are not supported.
mep *identifier*	1–8191	The MEP identifier to use for the measurement. The discovered MAC address for this MEP identifier is used.
maintenance-domain *name*	Existing MD name	Specifies an existing maintenance domain (MD) to use for the measurement.
maintenance-association *ma-id*	Existing MA identifier	Specifies an existing maintenance association (MA) identifier to use for the measurement.
count *count*	1–65535 (default: 10)	(Optional) Specifies the number of Ethernet frame delay frames to send. The default is 10.
wait *time*	1–255 seconds (default: 1)	(Optional) Specifies the number of seconds to wait between frames. The default is 1 second.

If you attempt to monitor delays to a nonexistent MAC address, you must exit the application manually using **^C**:

```
user@host> monitor ethernet delay-measurement two-way 00:11:22:33:44:55

Two-way ETH-DM request to 00:11:22:33:44:55, Interface ge-5/2/9.0
^C
--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 0
Average delay: 0 usec, Average delay variation: 0 usec
Best case delay: 0 usec, Worst case delay: 0 usec
```

SEE ALSO

Configuring Ethernet Frame Loss Measurement | 223

Starting an ETH-DM Session

IN THIS SECTION

- Using the monitor ethernet delay-measurement Command | 201
- Starting a One-Way ETH-DM Session | 202
- Starting a Two-Way ETH-DM Session | 203

Using the monitor ethernet delay-measurement Command

After you have configured two MX Series routers to support ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM), you can initiate a one-way or two-way Ethernet frame delay measurement session from the CFM maintenance association end point (MEP) on one of the routers to the peer MEP on the other router.

To start an ETH-DM session between the specified local MEP and the specified remote MEP, enter the **monitor ethernet delay-measurement** command at operational mode. The syntax of the command is as follows:

```
monitor ethernet delay-measurement
(one-way | two-way)
maintenance-domain md-name
maintenance-association ma-name
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<wait interval-seconds>
<priority 802.1p value>
<size>
<no-session-id-tlv>
<xml>
```

For a one-way frame delay measurement, the command displays a runtime display of the number of 1DM frames sent from the initiator MEP during that ETH-DM session. One-way frame delay and frame delay variation measurements from an ETH-DM session are collected in a CFM database at the router that contains the receiver MEP. You can retrieve ETH-DM statistics from a CFM database at a later time.

For a two-way frame delay measurement, the command displays two-way frame delay and frame delay variation values for each round-trip frame exchange during that ETH-DM session, as well as a runtime display of useful summary information about the session: average delay, average delay variation, best-case delay, and worst-case delay. Two-way frame delay and frame delay variation values measurements from

an ETH-DM session are collected in a CFM database at the router that contains the initiator MEP. You can retrieve ETH-DM statistics from a CFM database at a later time.

> **NOTE:** Although you can trigger frame delay collection for up to 65,535 ETH-DM requests at a time, a router stores only the last 100 frame delay statistics per CFM session (pair of peer MEPs).

For a complete description of the **monitor ethernet delay-measurement** operational command, see the CLI Explorer.

SEE ALSO

monitor ethernet delay-measurement | 2657

Starting a One-Way ETH-DM Session

To start a one-way Ethernet frame delay measurement session, enter the **monitor ethernet delay-measurement one-way** command from operational mode, and specify the peer MEP by its MAC address or by its MEP identifier.

For example:

`user@host>` **monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

> **NOTE:** If you attempt to monitor delays to a nonexistent MAC address, you must type **Ctrl + C** to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

SEE ALSO

monitor ethernet delay-measurement | 2657

Starting a Two-Way ETH-DM Session

To start a two-way Ethernet frame delay measurement session, enter the **monitor ethernet delay-measurement two-way** command from operational mode, and specify the peer MEP by its MAC address or by its MEP identifier.

For example:

`user@host>` **monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a Delay: 100 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 111 usec Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a Delay: 110 usec Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a Delay: 119 usec Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a Delay: 122 usec Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 108 usec Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

NOTE: If you attempt to monitor delays to a nonexistent MAC address, you must type **Ctrl + C** to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

SEE ALSO

monitor ethernet delay-measurement | 2657

SEE ALSO

Inline Transmission Mode | 300

Example: Configuring One-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces

This example uses two MX Series routers: **MX-1** and **MX-2**. The configuration creates a CFM down MEP session on a VLAN-tagged logical interface connecting the two (**ge-5/2/9** on Router **MX-1** and **ge-0/2/5** on Router **MX-2**).

> **NOTE:** These are not complete router configurations.

Configuration on Router **MX-1**:

```
[edit]
interfaces {
    ge-5/2/9 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
```

```
                }
                mep 201 {
                    interface ge-5/2/9.0;
                    direction down;
                    auto-discovery;
                }
            }
        }
    }
  }
}
```

Configuration on Router **MX-2**:

```
[edit]
interfaces {
    ge-0/2/5 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 101 {
```

```
                interface ge-0/2/5.0;
                direction down;
                auto-discovery;
              }
            }
          }
        }
      }
    }
  }
```

From Router **MX-2**, start a one-way delay measurement to Router **MX-1**.

`user@MX-2>` **monitor ethernet delay-measurement one-way mep 201 maintenance-domain md6 maintenance-association ma6 count 10**

```
One-way ETH-DM request to 00:90:69:0a:43:94, Interface ge-0/2/5.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

The counters are displayed as part of the local MEP database on Router **MX-2**.

`user@MX-2>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6 maintenance-domain ma6**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                 : no
    Erroneous CCM received                       : no
    Cross-connect CCM received                   : no
    RDI sent by some MEP                         : no
  Statistics:
    CCMs sent                                    : 1590
    CCMs received out of sequence                : 0
```

```
    LBMs sent                                       : 0
    Valid in-order LBRs received                    : 0
    Valid out-of-order LBRs received                : 0
    LBRs received with corrupted data               : 0
    LBRs sent                                       : 0
    LTMs sent                                       : 0
    LTMs received                                   : 0
    LTRs sent                                       : 0
    LTRs received                                   : 0
    Sequence number of next LTM request             : 0
    1DMs sent                                       : 10
    Valid 1DMs received                             : 0
    Invalid 1DMs received                           : 0
    DMMs sent                                       : 0
    DMRs sent                                       : 0
    Valid DMRs received                             : 0
    Invalid DMRs received                           : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      201     00:90:69:0a:43:94       ok    ge-0/2/5.0
```

The remote MEP database statistics are available on Router **MX-1**.

`user@MX-1>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: down, MAC address: 00:90:69:0a:43:94
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                    : no
    Erroneous CCM received                          : no
    Cross-connect CCM received                      : no
    RDI sent by some MEP                            : no
  Statistics:
    CCMs sent                                       : 1572
    CCMs received out of sequence                   : 0
    LBMs sent                                       : 0
    Valid in-order LBRs received                    : 0
    Valid out-of-order LBRs received                : 0
```

```
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 0
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 0
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 0
    Valid 1DMs received                           : 10
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      101     00:90:69:0a:48:57       ok    ge-5/2/9.0
```

The remote Router **MX-1** should also collect the delay statistics (up to 100 per session) for display with **mep-statistics** or **delay-statistics**.

`user@MX-1>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md6**

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
  CCMs sent                                     : 3240
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 0
  1DMs sent                                     : 0
  Valid 1DMs received                           : 10
  Invalid 1DMs received                         : 0
  DMMs sent                                     : 0
  DMRs sent                                     : 0
```

```
  Valid DMRs received                          : 0
  Invalid DMRs received                        : 0

  Remote MEP identifier: 101
  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        370
      2        357
      3        344
      4        332
      5        319
      6        306
      7        294
      8        281
      9        269
      10       255
    Average one-way delay          : 312 usec
    Average one-way delay variation: 11 usec
    Best case one-way delay        : 255 usec
    Worst case one-way delay       : 370 usec
```

user@MX-1> **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md6**

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1

  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        370
      2        357
      3        344
      4        332
      5        319
      6        306
      7        294
      8        281
      9        269
      10       255
```

```
Average one-way delay          : 312 usec
Average one-way delay variation: 11 usec
Best case one-way delay        : 255 usec
```

NOTE: When two systems are close to each other, their one-way delay values are very high compared to their two-way delay values. This is because one-way delay measurement requires the timing for the two systems to be synchronized at a very granular level and MX Series routers do not support this granular synchronization. However, two-way delay measurement does not require synchronized timing, making two-way delay measurements more accurate.

SEE ALSO

Ethernet Interfaces User Guide for Routing Devices

Ethernet Frame Delay Measurements Overview | **166**

Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements | **44**

Triggering an Ethernet Frame Delay Measurements Session | **199**

Viewing Ethernet Frame Delay Measurements Statistics | **217**

Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | **210**

Configuring ETH-DM with Untagged Interfaces

Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces

This example uses two MX Series routers: **MX-1** and **MX-2**. The configuration creates a CFM down MEP session on a VLAN-tagged logical interface connecting the two (**ge-5/2/9** on Router **MX-1** and **ge-0/2/5** on Router **MX-2**).

NOTE: These are not complete router configurations.

Configuration on Router **MX-1**:

```
[edit]
```

```
interfaces {
    ge-5/2/9 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 201 {
                            interface ge-5/2/9.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

Configuration on Router **MX-2**:

```
[edit]
interfaces {
    ge-0/2/5 {
```

```
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 101 {
                            interface ge-0/2/5.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

From Router **MX-1**, start a two-way delay measurement to Router **MX-2**.

`user@MX-1>` **monitor ethernet delay-measurement two-way mep 101 maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:90:69:0a:48:57, Interface ge-5/2/9.0
DMR received from 00:90:69:0a:48:57 Delay: 100 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 8 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 111 usec Delay variation: 19 usec
DMR received from 00:90:69:0a:48:57 Delay: 110 usec Delay variation: 1 usec
DMR received from 00:90:69:0a:48:57 Delay: 119 usec Delay variation: 9 usec
DMR received from 00:90:69:0a:48:57 Delay: 122 usec Delay variation: 3 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 30 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 108 usec Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

The counters are displayed as part of the MEP database on Router **MX-1** maintenance domain **MD6**.

`user@MX-1>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: down, MAC address: 00:90:69:0a:43:94
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                 : no
    Erroneous CCM received                       : no
    Cross-connect CCM received                   : no
    RDI sent by some MEP                         : no
  Statistics:
    CCMs sent                                    : 894
    CCMs received out of sequence                : 0
    LBMs sent                                    : 0
    Valid in-order LBRs received                 : 0
    Valid out-of-order LBRs received             : 0
    LBRs received with corrupted data            : 0
    LBRs sent                                    : 0
    LTMs sent                                    : 0
    LTMs received                                : 0
```

```
    LTRs sent                                      : 0
    LTRs received                                  : 0
    Sequence number of next LTM request            : 0
    1DMs sent                                      : 0
    Valid 1DMs received                            : 0
    Invalid 1DMs received                          : 0
    DMMs sent                                      : 10
    DMRs sent                                      : 0
    Valid DMRs received                            : 10
    Invalid DMRs received                          : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      101     00:90:69:0a:48:57       ok    ge-5/2/9.0
```

The collected MEP statistics are saved (up to 100 per remote MEP or per CFM session) and displayed as part of the MEP statistics on Router **MX-1**.

`user@MX-1>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md6**

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
  CCMs sent                                      : 3154
  CCMs received out of sequence                  : 0
  LBMs sent                                      : 0
  Valid in-order LBRs received                   : 0
  Valid out-of-order LBRs received               : 0
  LBRs received with corrupted data              : 0
  LBRs sent                                      : 0
  LTMs sent                                      : 0
  LTMs received                                  : 0
  LTRs sent                                      : 0
  LTRs received                                  : 0
  Sequence number of next LTM request            : 0
  1DMs sent                                      : 0
  Valid 1DMs received                            : 0
  Invalid 1DMs received                          : 0
  DMMs sent                                      : 10
  DMRs sent                                      : 0
  Valid DMRs received                            : 10
  Invalid DMRs received                          : 0

  Remote MEP identifier: 101
```

```
  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1                       100
      2                       92
      3                       92
      4                       111
      5                       110
      6                       119
      7                       122
      8                       92
      9                       92
      10                      108
    Average two-way delay          : 103 usec
    Average two-way delay variation: 8 usec
    Best case two-way delay        : 92 usec
    Worst case two-way delay       : 122 usec
```

The collected delay statistics are also saved (up to 100 per session) and displayed as part of the MEP delay statistics on Router **MX-1**.

`user@MX-1>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md6**

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1

  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
                          (usec)         (usec)
      1                      100
      2                      92
      3                      92
      4                      111
      5                      110
      6                      119
      7                      122
      8                      92
      9                      92
      10                     108
    Average two-way delay          : 103 usec
```

```
Average two-way delay variation: 8 usec
Best case two-way delay        : 92 usec
Worst case two-way delay       : 122 usec
```

SEE ALSO

Ethernet Interfaces User Guide for Routing Devices

Ethernet Frame Delay Measurements Overview | **166**

Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements | **44**

Triggering an Ethernet Frame Delay Measurements Session | **199**

Viewing Ethernet Frame Delay Measurements Statistics | **217**

Example: Configuring One-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces | **204**

Configuring ETH-DM with Untagged Interfaces

Managing Continuity Measurement Statistics

IN THIS SECTION

- Displaying Continuity Measurement Statistics | **216**
- Clearing Continuity Measurement Statistics | **217**

Displaying Continuity Measurement Statistics

Purpose

Display continuity measurement.

The **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1** command is enhanced to display continuity measurement statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

Action

- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1**

SEE ALSO

show oam ethernet connectivity-fault-management delay-statistics | 2679

Clearing Continuity Measurement Statistics

Purpose

Clear the continuity measurement statistics

By default, statistics are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

Action

- To clear the continuity measurement statistics for all MEPs attached to CFM-enabled interfaces on the router:

  `user@host>` **clear oam ethernet connectivity-fault-management continuity-measurement maintenance-domain *md-name* maintenance-association *ma-name* local-mep *local-mep-id* remote-mep *remote-mep-id***

SEE ALSO

clear oam ethernet connectivity-fault-management continuity-measurement | 2640

SEE ALSO

clear oam ethernet connectivity-fault-management continuity-measurement | 2640

show oam ethernet connectivity-fault-management delay-statistics | 2679

Viewing Ethernet Frame Delay Measurements Statistics

Once Ethernet frame delay measurement statistics have been collected, they can be displayed.

To retrieve the last 100 Ethernet frame delay measurement statistics per remote MEP or per CFM session, two types of **show** commands are provided:

- For all OAM frame counters and Ethernet frame delay measurement statistics
- For Ethernet frame delay measurement statistics only

To retrieve all Ethernet frame delay measurement statistics for a given session, use the **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain *name* maintenance-association *name* [local-mep *identifier*] [remote-mep *identifier*] [count *count*]** command.

To retrieve only Ethernet frame delay measurement statistics for a given session, use the **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain *name* maintenance-association *name* [local-mep *identifier*] [remote-mep *identifier*] [count *count*]** command.

> **NOTE:** The only difference in the two commands is the use of the **mep-statistics** and **delay-statistics** keyword.

The fields for these commands are described in Table 18 on page 218.

Table 18: Show Ethernet Delay Command Parameters

Parameter	Parameter Range	Description
maintenance-domain *name*	Existing MD name	Specifies an existing maintenance domain (MD) to use.
maintenance-association *ma-id*	Existing MA identifier	Specifies an existing maintenance association (MA) identifier to use.
local-mep *identifier*	1–8191	When a MEP has been specified, display statistics only for the local MEP.
remote-mep *identifier*	1–8191	When a MEP has been specified, display statistics only for the discovered MEP.
count *count*	1–100 (default:100)	The number of entries to display in the results table. By default, all 100 entries are displayed if they exist.

> **NOTE:** For each MEP, you will see frame counters for sent and received Ethernet frame delay measurement frames whenever MEP statistics are displayed.

SEE ALSO

Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40

Managing ETH-DM Statistics and ETH-DM Frame Counts

IN THIS SECTION

- Displaying ETH-DM Statistics Only | **219**
- Displaying ETH-DM Statistics and Frame Counts | **220**
- Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity | **220**
- Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level | **221**
- Clearing ETH-DM Statistics and Frame Counts | **222**

Displaying ETH-DM Statistics Only

Purpose

Display ETH-DM statistics.

By default, the **show oam ethernet connectivity-fault-management delay-statistics** command displays ETH-DM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

Action

- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain ma1 maintenance-association ma1**

- To display the ETH-DM statistics collected for ETH-DM sessions for the local MEP **201** belonging to MA **ma2** and within MD **md2**:

  `user@host>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md2 maintenance-association ma2 local-mep 201**

- To display the ETH-DM statistics collected for ETH-DM sessions from local MEPs belonging to MA **ma3** and within MD **md3** to remote MEP **302**:

  `user@host>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md3 maintenance-association ma3 remote-mep 302**

SEE ALSO

show oam ethernet connectivity-fault-management delay-statistics | 2679

Displaying ETH-DM Statistics and Frame Counts

Purpose

Display ETH-DM statistics and ETH-DM frame counts.

By default, the **show oam ethernet connectivity-fault-management mep-statistics** command displays ETH-DM statistics and frame counts for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

Action

- To display the ETH-DM statistics and ETH-DM frame counts for MEPs in MA **ma1** and within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma1**

- To display the ETH-DM statistics and ETH-DM frame counts for the local MEP **201** in MA **ma2** and within MD **md2**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md2 maintenance-association ma2 local-mep 201**

- To display the ETH-DM statistics and ETH-DM frame counts for the local MEP in MD **md3** and within MA **ma3** that participates in an ETH-DM session with the remote MEP **302**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain ma3 maintenance-association ma3 remote-mep 302**

SEE ALSO

show oam ethernet connectivity-fault-management mep-statistics | 2764

Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity

Purpose

Display ETH-DM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management mep-database** command displays CFM database information for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

NOTE: At the router attached to the initiator MEP for a one-way session, or at the router attached to the receiver MEP for a two-way session, you can only display ETH-DM frame counts.

Action

- To display CFM database information (including ETH-DM frame counts) for all MEPs in MA **ma1** within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain ma1 maintenance-association ma1**

- To display CFM database information (including ETH-DM frame counts) only for local MEP **201** in MA **ma1** within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md2 maintenance-association ma2 local-mep 201**

- To display CFM database information (including ETH-DM frame counts) only for remote MEP **302** in MD **md3** within MA **ma3**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain ma3 maintenance-association ma3 remote-mep 302**

SEE ALSO

show oam ethernet connectivity-fault-management mep-database | 2749

Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level

Purpose

Display ETH-DM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management interfaces** command displays CFM database information for MEPs attached to CFM-enabled Ethernet interfaces on the router or at a maintenance domain level. For Ethernet interfaces that support ETH-DM, any frame counts are also displayed when you specify the **detail** or **extensive** command option.

NOTE: At the router attached to the initiator MEP for a one-way session, or at the router attached to the receiver MEP for a two-way session, you can only display ETH-DM frame counts.

Action

- To display CFM database information (including ETH-DM frame counts) for all MEPs attached to CFM-enabled Ethernet interfaces on the router:

  ```
  user@host> show oam ethernet connectivity-fault-management interfaces detail
  ```

- To display CFM database information (including ETH-DM frame counts) only for the MEPs attached to CFM-enabled router interface **ge-5/2/9.0**:

  ```
  user@host> show oam ethernet connectivity-fault-management interfaces ge-5/2/9.0 detail
  ```

- To display CFM database information (including ETH-DM frame counts) only for MEPs enclosed within CFM maintenance domains (MDs) at level **6**:

  ```
  user@host> show oam ethernet connectivity-fault-management interfaces level 6 detail
  ```

SEE ALSO

show oam ethernet connectivity-fault-management interfaces | 2727

Clearing ETH-DM Statistics and Frame Counts

Purpose

Clear the ETH-DM statistics and ETH-DM frame counts.

By default, statistics and frame counts are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

Action

- To clear the ETH-DM statistics and ETH-DM frame counts for all MEPs attached to CFM-enabled interfaces on the router:

  ```
  user@host> clear oam ethernet connectivity-fault-management statistics
  ```

- To clear the ETH-DM statistics and ETH-DM frame counts only for MEPs attached to the logical interface **ge-0/5.9.0**:

  ```
  user@host> clear oam ethernet connectivity-fault-management statistics ge-0/5/9.0
  ```

SEE ALSO

clear oam ethernet connectivity-fault-management statistics | 2647

SEE ALSO

- clear oam ethernet connectivity-fault-management statistics | 2647
- show oam ethernet connectivity-fault-management delay-statistics | 2679
- show oam ethernet connectivity-fault-management interfaces | 2727
- show oam ethernet connectivity-fault-management mep-statistics | 2764
- show oam ethernet connectivity-fault-management mep-database | 2749

RELATED DOCUMENTATION

- Configuring an Iterator Profile | 257
- Configuring Ethernet Synthetic Loss Measurements | 272
- Ethernet Alarm Indication | 286
- Inline Transmission Mode | 300

Configuring Ethernet Frame Loss Measurement

IN THIS SECTION

- Configuring Statistical Frame Loss Measurement for VPLS Connections | 223
- Managing ETH-LM Statistics | 224
- Example: Measuring Ethernet Frame Loss for Single-Tagged LMM/LMR PDUs | 226
- Example: Measuring Ethernet Frame Loss for Dual-Tagged LMM/LMR PDUs | 242

Use this topic to understand more about frame loss measurement and how to configure frame loss measurement.

Configuring Statistical Frame Loss Measurement for VPLS Connections

Using proactive statistical frame loss measurement, you can monitor VPLS connections on MX Series routers . Statistical frame loss measurement allows you to monitor the quality of Ethernet connections for service level agreements (SLAs). Point-to-point and multipoint-to-multipoint connections configured on MX Series routers can be monitored by registering the connection on an iterator and initiating periodic SLA measurement of frame transmissions on the connections.

Iterators periodically transmit SLA measurement packets using ITU-Y.1731 compliant frames. The iterator sends periodic measurement packets for each of the connections registered to it. These measurement cycles are transmitted in such a way as to not overlap, reducing the processing demands placed on the CPU. The measurement packets are exchanged between the source user network interface (UNI) port and the destination UNI port, providing a sequence of timed performance measurements for each UNI pair. The Frame Loss Ratio (FLR) and connection availability can be computed from these measurements using statistics.

The following steps outline how to configure statistical frame loss measurement for VPLS connections:

1. To configure proactive ETH-DM measurement for a VPLS connection, see "Guidelines for Configuring Routers to Support an ETH-DM Session" on page 186.

2. To enable statistical loss measurement for a VPLS connection, configure an iterator for the VPLS connection using the **sla-iterator-profiles** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level. For detailed instructions, see "Configuring an Iterator Profile" on page 258.

3. As part of the iterator configuration, include the **statistical-frame-loss** option for the **measurement-type** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles *profile-name*]** hierarchy level.

4. Once you have enabled the iterator, you can display the statistical frame loss for a VPLS connection by issuing the **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator *identifier* maintenance-domain *name* maintenance-association *name* local-mep *identifier* remote-mep *identifier*** command.

SEE ALSO

Configuring an Iterator Profile | 258

Verifying the Configuration of an Iterator Profile | 261

Managing ETH-LM Statistics

IN THIS SECTION

- Displaying ETH-LM Statistics | 225
- Clearing ETH-LM Statistics | 226

Displaying ETH-LM Statistics

Purpose

Display the ETH-LM statistics.

By default, the **show oam ethernet connectivity-fault-management loss-statistics maintenance-domain *md-name* maintenance-association *ma-name*** command displays ETH-LM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

The following list consists of the CFM-related operational mode commands that have been enhanced to display ETH-LM statistics:

- The **show oam ethernet connectivity-fault-management interfaces detail** command is enhanced to display ETH-DM and ETH-LM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).
- The **show oam ethernet connectivity-fault-management mep-statistics** command is enhanced to display ETH-DM and ETH-LM statistics and frame counts for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).
- The **show oam ethernet connectivity-fault-management mep-database** command is enhanced to display ETH-DM and ETH-LM frame counters for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

Action

- To display the ETH-LM statistics for all MEPs attached to CFM-enabled interfaces on the router:

  `user@host>` **show oam ethernet connectivity-fault-management loss-statistics**

- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1**

- To display the ETH-DM statistics and ETH-DM frame counts for MEPs in MA **ma1** and within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma1**

- To display CFM database information (including ETH-DM frame counts) for all MEPs in MA **ma1** within MD **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md1 maintenance-association ma1**

SEE ALSO

- clear oam ethernet connectivity-fault-management loss-statistics | 2643
- show oam ethernet connectivity-fault-management delay-statistics | 2679
- show oam ethernet connectivity-fault-management interfaces | 2727 (**detail** | **extensive**)
- show oam ethernet connectivity-fault-management mep-statistics | 2764
- show oam ethernet connectivity-fault-management mep-database | 2749
- show oam ethernet connectivity-fault-management loss-statistics | 2744

Clearing ETH-LM Statistics

Purpose

Clear the ETH-LM statistics.

By default, statistics are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

Action

- To clear the ETH-LM statistics for all MEPs attached to CFM-enabled interfaces on the router:

```
user@host> clear oam ethernet connectivity-fault-management loss-statistics
```

SEE ALSO

- clear oam ethernet connectivity-fault-management loss-statistics | 2643

SEE ALSO

- Managing ETH-DM Statistics and ETH-DM Frame Counts | 219

Example: Measuring Ethernet Frame Loss for Single-Tagged LMM/LMR PDUs

IN THIS SECTION

- Requirements | 227
- Overview and Topology | 227
- Configuration | 228
- Verification | 239

This example illustrates how to configure Ethernet frame loss measurement (ETH-LM) for single-tagged Loss Measurement Message (LMM)/Loss Measurement Reply (LMR) protocol data units (PDUs). By configuring ETH-LM, you can measure the Ethernet frame loss that occur in your network.

Requirements

This example uses the following hardware and software components:

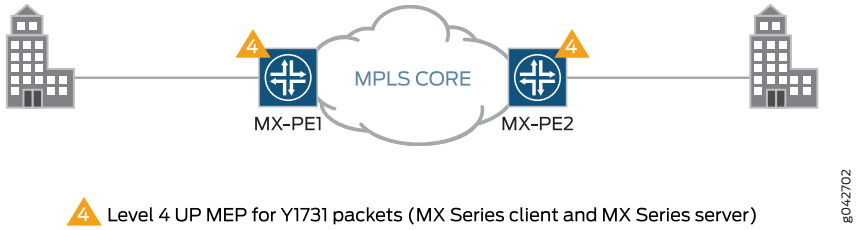
- Two MX Series 5G Universal Routing Platforms with Rev-B Dense Port Concentrators (DPCs)
- Junos OS Release 14.2 or later

Overview and Topology

Junos OS supports Ethernet frame loss measurement (ETH-LM) between maintenance association end points (MEPs) configured on Ethernet physical or logical interfaces on Rev-B Dense Port Concentrators (DPCs) in MX Series routers. Additionally, the Y.1731 functionality supports ETH-LM only for an end-to-end connection that uses Virtual Private Wire Service (VPWS). This example illustrates how to configure ETH-LM for single-tagged LMM/LMR PDUs with input and output VLAN map configured as **swap**.

Figure 18 on page 227 shows the topology used in this example. VPWS service is configured between two MX Series routers, MX-PE1 and MX PE2.

Figure 18: VPWS Service Configured Between Two MX Series Routers



MX-PE1 router has two Ethernet interfaces, **ge-5/0/4** and **ge-5/1/9**. Virtual LAN (VLAN) is configured on **ge-5/0/4** and MPLS is configured on the **ge-5/1/9** interface. The **ge-5/0/4.11** interface is used to configure the Layer 2 virtual circuit with MX-PE2 router. The UP MEP, **mep 2**, is attached to the **ge-5/0/4.11** interface. The three-color policer firewall filter is also configured for the MX-PE1 router.

Similarly, MX-PE2 router has two Ethernet interfaces, **ge-8/0/8** and **ge-8/0/9**. Virtual LAN (VLAN) is configured on **ge-8/0/8** and MPLS is configured on the **ge-8/0/9** interface. The **ge-8/0/8.11** interface is used to configure the Layer 2 virtual circuit with MX-PE1 router. The UP MEP, **mep 1**, is attached to the **ge-8/0/8.11** interface. The three-color policer firewall filter is also configured for the MX-PE2 router.

Configuration

IN THIS SECTION

- Configuring Router PE1 | 230
- Configuring Router PE2 | 235

CLI Quick Configuration

To quickly configure ETH-LM for single-tagged LMM/LMR PDUs, copy the following commands, remove any line breaks, and then paste the commands into the CLI of each device.

On Router PE1:

```
[edit]
set interfaces ge-5/0/4 encapsulation flexible-ethernet-services
set interfaces ge-5/0/4 unit 11 encapsulation vlan-ccc
set interfaces ge-5/0/4 unit 11 layer2-policer input-three-color abc
set interfaces ge-5/0/4 unit 11 family ccc
set interfaces ge-5/1/9 enable
set interfaces ge-5/1/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-5/1/9 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set interfaces ge-5/0/4 flexible-vlan-tagging
set interfaces ge-5/0/4 unit 11 vlan-id 2000
set interfaces ge-5/0/4 unit 11 input-vlan-map swap
set interfaces ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-5/0/4 unit 11 output-vlan-map swap
set routing-options router-id 4.4.4.4
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
set protocols oam ethernet connectivity-fault-management performance-monitoring delegate-server-processing
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 2 interface ge-5/0/4.11
```

```
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
    ma mep 2 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
    ma mep 2 remote-mep 1
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

On Router PE2:

```
[edit]
set interfaces ge-8/0/8 encapsulation flexible-ethernet-services
set interfaces ge-8/0/8 unit 11 encapsulation vlan-ccc
set interfaces ge-8/0/8 unit 11 layer2-policer input-three-color abc
set interfaces ge-8/0/8 unit 11 family ccc
set interfaces ge-8/0/9 enable
set interfaces ge-8/0/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-8/0/9 unit 0 family mpls
set interfaces ae0 unit 0 family inet
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces ge-8/0/8 flexible-vlan-tagging
set interfaces ge-8/0/8 unit 11 vlan-id 2000
set interfaces ge-8/0/8 unit 11 input-vlan-map swap
set interfaces ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-8/0/8 unit 11 output-vlan-map swap
set routing-options router-id 3.3.3.3
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
    ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
    ma mep 1 interface ge-8/0/8.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
    ma mep 1 direction up
```

```
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 1 remote-mep 2
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

Configuring Router PE1

Step-by-Step Procedure

To configure Router PE1:

1. Configure the interfaces.

```
[edit]
user@PE1# edit interfaces
[edit interfaces]
user@PE1# set ge-5/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-5/0/4 unit 11 encapsulation vlan-ccc
user@PE1# set ge-5/0/4 unit 11 layer2-policer input-three-color abc
user@PE1# set ge-5/0/4 unit 11 family ccc
user@PE1# set ge-5/1/9 enable
user@PE1# set ge-5/1/9 unit 0 family inet address 12.1.1.1/24
user@PE1# set ge-5/1/9 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 4.4.4.4/32
```

2. Configure the VLAN.

```
[edit interfaces]
user@PE1# set ge-5/0/4 flexible-vlan-tagging
user@PE1# set ge-5/0/4 unit 11 vlan-id 2000
user@PE1# set ge-5/0/4 unit 11 input-vlan-map swap
user@PE1# set ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
user@PE1# set ge-5/0/4 unit 11 output-vlan-map swap
```

3. Configure the router identifier to identify the routing device.

```
[edit]
user@PE1# edit routing-options
```

```
[edit routing-options]
user@PE1# set router-id 4.4.4.4
```

4. Configure MPLS, OSPF, and LDP protocols.

```
[edit]
user@PE1# edit protocols
[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
```

5. Configure the Layer 2 circuit.

```
[edit protocols]
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
```

6. Configure the MEP.

```
[edit protocols]
user@PE1# set oam ethernet connectivity-fault-management performance-monitoring
   delegate-server-processing
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma continuity-check interval 1s
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 interface ge-5/0/4.11
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 direction up
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 remote-mep 1
```

7. Configure the firewall.

```
[edit]
```

```
user@PE1# edit firewall
[edit firewall]
user@PE1# set three-color-policer abc logical-interface-policer
user@PE1# set three-color-policer abc two-rate color-blind
user@PE1# set three-color-policer abc two-rate committed-information-rate 10m
user@PE1# set three-color-policer abc two-rate committed-burst-size 1500
user@PE1# set three-color-policer abc two-rate peak-information-rate 20m
user@PE1# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Commit the configuration.

```
[edit]
user@PE1# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-options**, and **show firewall** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show interfaces
interfaces {
    ge-5/0/4 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-id 2000;
            input-vlan-map {
                swap;
                vlan-id 4094;
            }
            output-vlan-map swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
    ge-5/1/9 {
        enable;
        unit 0 {
```

```
        family inet {
            address 12.1.1.1/24;
        }
        family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 4.4.4.4/32;
      }
    }
  }
}
```

```
user@PE1# show protocols
protocols {
  mpls {
    interface all;
    interface fxp0.0 {
      disable;
    }
  }
  ospf {
    area 0.0.0.0 {
      interface all;
      interface fxp0.0 {
        disable;
      }
    }
  }
  ldp {
    interface all;
    interface fxp0.0 {
      disable;
    }
  }
  l2circuit {
    neighbor 3.3.3.3 {
      interface ge-5/0/4.11 {
        virtual-circuit-id 1003;
        no-control-word;
      }
    }
```

```
    }
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    delegate-server-processing;
                }
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 2 {
                            interface ge-5/0/4.11;
                            direction up;
                            remote-mep 1;
                        }
                    }
                }
            }
        }
    }
}
```

```
user@PE1# show routing-options
routing-options {
    router-id 4.4.4.4;
}
```

```
user@PE1# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Configuring Router PE2

Step-by-Step Procedure

To configure Router PE2:

1. Configure the interfaces.

```
[edit]
user@PE2# edit interfaces
[edit interfaces]
user@PE2# set ge-8/0/8 encapsulation flexible-ethernet-services
user@PE2# set ge-8/0/8 unit 11 encapsulation vlan-ccc
user@PE2# set ge-8/0/8 unit 11 layer2-policer input-three-color abc
user@PE2# set ge-8/0/8 unit 11 family ccc
user@PE2# set ge-8/0/9 enable
user@PE2# set ge-8/0/9 unit 0 family inet address 12.1.1.1/24
user@PE2# set ge-8/0/9 unit 0 family mpls
user@PE2# set ae0 unit 0 family inet
user@PE2# set lo0 unit 0 family inet address 3.3.3.3/32
```

2. Configure the VLAN.

```
[edit interfaces]
user@PE2# set ge-8/0/8 flexible-vlan-tagging
user@PE2# set ge-8/0/8 unit 11 vlan-id 2000
user@PE2# set ge-8/0/8 unit 11 input-vlan-map swap
user@PE2# set ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
user@PE2# set ge-8/0/8 unit 11 output-vlan-map swap
```

3. Configure the router identifier to identify the routing device.

```
[edit]
user@PE2# edit routing-options
[edit routing-options]
user@PE2# set router-id 3.3.3.3
```

4. Configure MPLS, OSPF, and LDP protocols.

```
[edit]
user@PE2# edit protocols
[edit protocols]
```

```
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set ospf area 0.0.0.0 interface all
user@PE2# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable
```

5. Configure the Layer 2 circuit.

```
[edit protocols]
user@PE2# set l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
user@PE2# set l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
```

6. Configure the MEP.

```
[edit protocols]
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma continuity-check interval 1s
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 interface ge-8/0/8.11
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 direction up
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 remote-mep 2
```

7. Configure the firewall.

```
[edit]
user@PE2# edit firewall
[edit firewall]
user@PE2# set three-color-policer abc logical-interface-policer
user@PE2# set three-color-policer abc two-rate color-blind
user@PE2# set three-color-policer abc two-rate committed-information-rate 10m
user@PE2# set three-color-policer abc two-rate committed-burst-size 1500
user@PE2# set three-color-policer abc two-rate peak-information-rate 20m
user@PE2# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Commit the configuration.

```
[edit]
user@PE2# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-options**, and **show firewall** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE2# show interfaces
interfaces {
    ge-8/0/8 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-id 2000;
            input-vlan-map {
                swap;
                vlan-id 4094;
            }
            output-vlan-map swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
    ge-8/0/9 {
        unit 0 {
            family inet {
                address 12.1.1.2/24;
            }
            family mpls;
        }
    }
    ae0 {
        unit 0 {
            family inet;
        }
    }
    lo0 {
```

```
        unit 0 {
            family inet {
                address 3.3.3.3/32;
            }
        }
    }
}
```

```
user@PE2# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    l2circuit {
        neighbor 4.4.4.4 {
            interface ge-8/0/8.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
```

```
                continuity-check {
                    interval 1s;
                }
                mep 1 {
                    interface ge-8/0/8.11;
                    direction up;
                    remote-mep 2;
                }
            }
        }
    }
  }
}
```

```
user@PE2# show routing-options
routing-options {
    router-id 3.3.3.3;
}
```

```
user@PE2# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Verification

IN THIS SECTION

- Viewing ETH-LM | 240

To start monitoring the Ethernet frame loss, issue the **monitor ethernet loss-measurement maintenance-domain md maintenance-association ma mep 1** command. Frame loss is calculated by collecting the counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the **monitor ethernet loss-measurement** command. You can also issue the **show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11** command to display ETH-LM statistics.

Viewing ETH-LM

Purpose

View the ETH-LM statistics.

Action

From operational mode, enter the **show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11** command.

```
user@PE1> show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11

Interface name: ge-5/0/4.11 , Interface status: Active, Link status: Up
  Maintenance domain name: md, Format: string, Level: 4
    Maintenance association name: ma, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: no
    MEP identifier: 2, Direction: up, MAC address: 00:24:dc:9b:96:76
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : no
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : no
      Some remote MEP's MAC in error state         : no
    Statistics:
      CCMs sent                                    : 36
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
      LBRs received with corrupted data            : 0
      LBRs sent                                    : 0
      LTMs sent                                    : 0
      LTMs received                                : 0
      LTRs sent                                    : 0
      LTRs received                                : 0
```

```
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 0
    Valid 1DMs received                           : 0
    Invalid 1DMs received                         : 0
    Out of sync 1DMs received                     : 0
    DMMs sent                                     : 0
    Valid DMMs received                           : 0
    Invalid DMMs received                         : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
    LMMs sent                                     : 10
    Valid LMMs received                           : 0
    Invalid LMMs received                         : 0
    LMRs sent                                     : 0
    Valid LMRs received                           : 10
    Invalid LMRs received                         : 0
    SLMs sent                                     : 0
    Valid SLMs received                           : 0
    Invalid SLMs received                         : 0
    SLRs sent                                     : 0
    Valid SLRs received                           : 0
    Invalid SLRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
        1     00:05:85:76:e5:30       ok    ge-5/0/4.11
```

Meaning

The Ethernet interface details and statistics are displayed. This output indicates that the **ge-5/0/4.11** interface is active and its link status is **up**. Its maintenance domain name is **md** and its level is **4**. The MEP identifier of the **ge-5/0/4.11** interface is indicated as **2** and its direction is **up**. Under the statistics section, the output indicates that **10** LMMs were sent and **10** valid LMRs were received by the interface.

SEE ALSO

Configuring Ethernet Synthetic Loss Measurements | 272

Introduction to OAM Connectivity Fault Management (CFM) | 22

Example: Measuring Ethernet Frame Loss for Dual-Tagged LMM/LMR PDUs

IN THIS SECTION

- Requirements | 242
- Overview and Topology | 242
- Configuration | 243
- Verification | 255

This example illustrates how to configure Ethernet frame loss measurement (ETH-LM) for dual-tagged Loss Measurement Message (LMM)/Loss Measurement Reply (LMR) protocol data units (PDUs). By configuring ETH-LM, you can measure the Ethernet frame loss that occur in your network.

Requirements

This example uses the following hardware and software components:

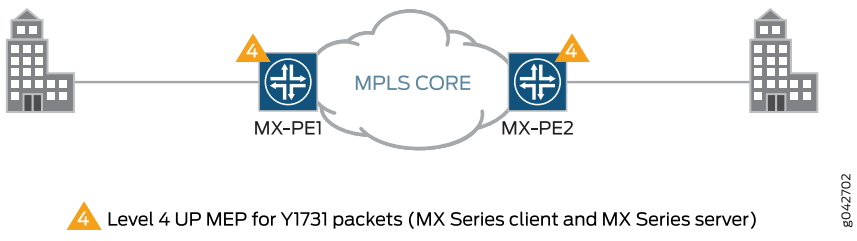
- Two MX Series 5G Universal Routing Platforms with Rev-B Dense Port Concentrators (DPCs)
- Junos OS Release 14.2 or later

Overview and Topology

Junos OS supports Ethernet frame loss measurement (ETH-LM) between maintenance association end points (MEPs) configured on Ethernet physical or logical interfaces on Rev-B Dense Port Concentrators (DPCs) in MX Series routers. Additionally, the Y.1731 functionality supports ETH-LM only for an end-to-end connection that uses Virtual Private Wire Service (VPWS). This example illustrates how to configure ETH-LM for dual tagged LMM/LMR PDUs with input and output VLAN map configured as **swap-swap**.

Figure 19 on page 242 shows the topology used in this example. VPWS service is configured between two MX Sereies routers, MX-PE1 and MX PE2.

Figure 19: VPWS Service Configured Between Two MX Series Routers



MX-PE1 router has two Ethernet interfaces, **ge-5/0/4** and **ge-5/1/9**. Virtual LAN (VLAN) is configured on **ge-5/0/4** and MPLS is configured on the **ge-5/1/9** interface. The **ge-5/0/4.11** interface is used to configure the Layer 2 virtual circuit with MX-PE2 router. The UP MEP, **mep 2**, is attached to the **ge-5/0/4.11** interface. The three-color policer firewall filter is also configured for the MX-PE1 router.

Similarly, MX-PE2 router has two Ethernet interfaces, **ge-8/0/8** and **ge-8/0/9**. Virtual LAN (VLAN) is configured on **ge-8/0/8** and MPLS is configured on the **ge-8/0/9** interface. The **ge-8/0/8.11** interface is used to configure the Layer 2 virtual circuit with MX-PE1 router. The UP MEP, **mep 1**, is attached to the **ge-8/0/8.11** interface. The three-color policer firewall filter is also configured for the MX-PE2 router.

Configuration

IN THIS SECTION

- Configuring Router PE1 | **245**
- Configuring Router PE2 | **250**

CLI Quick Configuration

To quickly configure ETH-LM for dual tagged LMM/LMR PDUs, copy the following commands, remove any line breaks, and then paste the commands into the CLI of each device.

On Router PE1:

```
[edit]
set interfaces ge-5/0/4 encapsulation flexible-ethernet-services
set interfaces ge-5/0/4 unit 11 encapsulation vlan-ccc
set interfaces ge-5/0/4 unit 11 layer2-policer input-three-color abc
set interfaces ge-5/0/4 unit 11 family ccc
set interfaces ge-5/1/9 enable
set interfaces ge-5/1/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-5/1/9 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set interfaces ge-5/0/4 flexible-vlan-tagging
set interfaces ge-5/0/4 unit 11 vlan-tags outer 2000 inner 1000
set interfaces ge-5/0/4 unit 11 input-vlan-map swap-swap
set interfaces ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-5/0/4 unit 11 input-vlan-map inner-vlan-id 4093
set interfaces ge-5/0/4 unit 11 output-vlan-map swap-swap
set routing-options router-id 4.4.4.4
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

```
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
set protocols oam ethernet connectivity-fault-management performance-monitoring delegate-server-processing
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 2 interface ge-5/0/4.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 2 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 2 remote-mep 1
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

On Router PE2:

```
[edit]
set interfaces ge-8/0/8 encapsulation flexible-ethernet-services
set interfaces ge-8/0/8 unit 11 encapsulation vlan-ccc
set interfaces ge-8/0/8 unit 11 layer2-policer input-three-color abc
set interfaces ge-8/0/8 unit 11 family ccc
set interfaces ge-8/0/9 enable
set interfaces ge-8/0/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-8/0/9 unit 0 family mpls
set interfaces ae0 unit 0 family inet
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces ge-8/0/8 flexible-vlan-tagging
set interfaces ge-8/0/8 unit 11 vlan-tags outer 2000 inner 1000
set interfaces ge-8/0/8 unit 11 input-vlan-map swap-swap
set interfaces ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-8/0/8 unit 11 input-vlan-map inner-vlan-id 4093
set interfaces ge-8/0/8 unit 11 output-vlan-map swap-swap
set routing-options router-id 3.3.3.3
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

```
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 1 interface ge-8/0/8.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 1 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association
   ma mep 1 remote-mep 2
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

Configuring Router PE1

Step-by-Step Procedure

To configure Router PE1:

1. Configure the interfaces.

```
[edit]
user@PE1# edit interfaces
[edit interfaces]
user@PE1# set ge-5/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-5/0/4 unit 11 encapsulation vlan-ccc
user@PE1# set ge-5/0/4 unit 11 layer2-policer input-three-color abc
user@PE1# set ge-5/0/4 unit 11 family ccc
user@PE1# set ge-5/1/9 enable
user@PE1# set ge-5/1/9 unit 0 family inet address 12.1.1.1/24
user@PE1# set ge-5/1/9 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 4.4.4.4/32
```

2. Configure the VLAN.

```
[edit interfaces]
user@PE1# set ge-5/0/4 flexible-vlan-tagging
```

```
user@PE1# set ge-5/0/4 unit 11 vlan-tags outer 2000 inner 1000
user@PE1# set ge-5/0/4 unit 11 input-vlan-map swap-swap
user@PE1# set ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
user@PE1# set ge-5/0/4 unit 11 input-vlan-map inner-vlan-id 4093
user@PE1# set ge-5/0/4 unit 11 output-vlan-map swap-swap
```

3. Configure the router identifier to identify the routing device.

```
[edit]
user@PE1# edit routing-options
[edit routing-options]
user@PE1# set router-id 4.4.4.4
```

4. Configure MPLS, OSPF, and LDP protocols.

```
[edit]
user@PE1# edit protocols
[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
```

5. Configure the Layer 2 circuit.

```
[edit protocols]
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
```

6. Configure the MEP.

```
[edit protocols]
user@PE1# set oam ethernet connectivity-fault-management performance-monitoring
   delegate-server-processing
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma continuity-check interval 1s
```

```
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 interface ge-5/0/4.11
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 direction up
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 2 remote-mep 1
```

7. Configure the firewall.

```
[edit]
user@PE1# edit firewall
[edit firewall]
user@PE1# set three-color-policer abc logical-interface-policer
user@PE1# set three-color-policer abc two-rate color-blind
user@PE1# set three-color-policer abc two-rate committed-information-rate 10m
user@PE1# set three-color-policer abc two-rate committed-burst-size 1500
user@PE1# set three-color-policer abc two-rate peak-information-rate 20m
user@PE1# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Commit the configuration.

```
[edit]
user@PE1# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-options**, and **show firewall** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show interfaces
interfaces {
   ge-5/0/4 {
      flexible-vlan-tagging;
      encapsulation flexible-ethernet-services;
      unit 11 {
         encapsulation vlan-ccc;
         vlan-tags outer 2000 inner 1000;
         input-vlan-map {
            swap-swap;
            vlan-id 4094;
```

```
            inner-vlan-id 4093;
        }
        output-vlan-map swap-swap;
        layer2-policer {
            input-three-color abc;
        }
        family ccc;
    }
}
ge-5/1/9 {
    enable;
    unit 0 {
        family inet {
            address 12.1.1.1/24;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 4.4.4.4/32;
        }
    }
}
}
```

```
user@PE1# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
```

```
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    l2circuit {
        neighbor 3.3.3.3 {
            interface ge-5/0/4.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    delegate-server-processing;
                }
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 2 {
                            interface ge-5/0/4.11;
                            direction up;
                            remote-mep 1;
                        }
                    }
                }
            }
        }
    }
}
```

```
user@PE1# show routing-options
routing-options {
    router-id 4.4.4.4;
}
```

```
user@PE1# show firewall
```

```
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Configuring Router PE2

Step-by-Step Procedure

To configure Router PE2:

1. Configure the interfaces.

```
[edit]
user@PE2# edit interfaces
[edit interfaces]
user@PE2# set ge-8/0/8 encapsulation flexible-ethernet-services
user@PE2# set ge-8/0/8 unit 11 encapsulation vlan-ccc
user@PE2# set ge-8/0/8 unit 11 layer2-policer input-three-color abc
user@PE2# set ge-8/0/8 unit 11 family ccc
user@PE2# set ge-8/0/9 enable
user@PE2# set ge-8/0/9 unit 0 family inet address 12.1.1.1/24
user@PE2# set ge-8/0/9 unit 0 family mpls
user@PE2# set ae0 unit 0 family inet
user@PE2# set lo0 unit 0 family inet address 3.3.3.3/32
```

2. Configure the VLAN.

```
[edit interfaces]
user@PE2# set ge-8/0/8 flexible-vlan-tagging
user@PE2# set ge-8/0/8 unit 11 vlan-tags outer 2000 inner 1000
user@PE2# set ge-8/0/8 unit 11 input-vlan-map swap-swap
user@PE2# set ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
user@PE2# set ge-8/0/8 unit 11 input-vlan-map inner-vlan-id 4093
user@PE2# set ge-8/0/8 unit 11 output-vlan-map swap-swap
```

3. Configure the router identifier to identify the routing device.

```
[edit]
user@PE2# edit routing-options
[edit routing-options]
user@PE2# set router-id 3.3.3.3
```

4. Configure MPLS, OSPF, and LDP protocols.

```
[edit]
user@PE2# edit protocols
[edit protocols]
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set ospf area 0.0.0.0 interface all
user@PE2# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable
```

5. Configure the Layer 2 circuit.

```
[edit protocols]
user@PE2# set l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
user@PE2# set l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
```

6. Configure the MEP.

```
[edit protocols]
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma continuity-check interval 1s
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 interface ge-8/0/8.11
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 direction up
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md
   maintenance-association ma mep 1 remote-mep 2
```

7. Configure the firewall.

```
[edit]
user@PE2# edit firewall
[edit firewall]
user@PE2# set three-color-policer abc logical-interface-policer
user@PE2# set three-color-policer abc two-rate color-blind
user@PE2# set three-color-policer abc two-rate committed-information-rate 10m
user@PE2# set three-color-policer abc two-rate committed-burst-size 1500
user@PE2# set three-color-policer abc two-rate peak-information-rate 20m
user@PE2# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Commit the configuration.

```
[edit]
user@PE2# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-options**, and **show firewall** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE2# show interfaces
interfaces {
    ge-8/0/8 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-tags outer 2000 inner 1000;
            input-vlan-map {
                swap-swap;
                vlan-id 4094;
                inner-vlan-id 4093;
            }
            output-vlan-map swap-swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
```

```
    ge-8/0/9 {
        unit 0 {
            family inet {
                address 12.1.1.2/24;
            }
            family mpls;
        }
    }
    ae0 {
        unit 0 {
            family inet;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.3/32;
            }
        }
    }
}
```

```
user@PE2# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
```

```
    l2circuit {
        neighbor 4.4.4.4 {
            interface ge-8/0/8.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 1 {
                            interface ge-8/0/8.11;
                            direction up;
                            remote-mep 2;
                        }
                    }
                }
            }
        }
    }
}
```

```
user@PE2# show routing-options
routing-options {
    router-id 3.3.3.3;
}
```

```
user@PE2# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
```

```
        peak-burst-size 15k;
      }
    }
  }
```

Verification

IN THIS SECTION

- Viewing ETH-LM | **255**

To start the Ethernet frame loss measurement session, issue the **monitor ethernet loss-measurement maintenance-domain md maintenance-association ma mep 1** command. Frame loss is calculated by collecting the counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the **monitor ethernet loss-measurement** command. You can also issue the **show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11** command to display ETH-LM statistics.

Viewing ETH-LM

Purpose

View the ETH-LM statistics.

Action

From operational mode, enter the **show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11** command.

```
user@PE1> show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11
```

```
Interface name: ge-5/0/4.11 , Interface status: Active, Link status: Up
  Maintenance domain name: md, Format: string, Level: 4
    Maintenance association name: ma, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: no
    MEP identifier: 2, Direction: up, MAC address: 00:24:dc:9b:96:76
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                : no
      Erroneous CCM received                      : no
```

```
  Cross-connect CCM received                    : no
  RDI sent by some MEP                          : no
  Some remote MEP's MAC in error state          : no
Statistics:
  CCMs sent                                     : 59
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 0
  1DMs sent                                     : 0
  Valid 1DMs received                           : 0
  Invalid 1DMs received                         : 0
  Out of sync 1DMs received                     : 0
  DMMs sent                                     : 0
  Valid DMMs received                           : 0
  Invalid DMMs received                         : 0
  DMRs sent                                     : 0
  Valid DMRs received                           : 0
  Invalid DMRs received                         : 0
  LMMs sent                                     : 10
  Valid LMMs received                           : 0
  Invalid LMMs received                         : 0
  LMRs sent                                     : 0
  Valid LMRs received                           : 10
  Invalid LMRs received                         : 0
  SLMs sent                                     : 0
  Valid SLMs received                           : 0
  Invalid SLMs received                         : 0
  SLRs sent                                     : 0
  Valid SLRs received                           : 0
  Invalid SLRs received                         : 0
Remote MEP count: 1
  Identifier    MAC address        State    Interface
      1     00:05:85:76:e5:30       ok    ge-5/0/4.11
```

Meaning

The Ethernet interface details and statistics are displayed. This output indicates that the **ge-5/0/4.11** interface is active and its link status is **up**. Its maintenance domain name is **md** and its level is **4**. The MEP identifier of the **ge-5/0/4.11** interface is indicated as **2** and its direction is **up**. Under the statistics section, the output indicates that **10** LMMs were sent and **10** valid LMRs were received by the interface.

SEE ALSO

Configuring Ethernet Synthetic Loss Measurements | 272
Introduction to OAM Connectivity Fault Management (CFM) | 22

RELATED DOCUMENTATION

ITU-T Y.1731 Ethernet Service OAM Overview | 165
Configuring Ethernet Synthetic Loss Measurements | 272

Configuring an Iterator Profile

IN THIS SECTION

- Configuring an Iterator Profile | 258
- Verifying the Configuration of an Iterator Profile | 261
- Managing Iterator Statistics | 264
- Configuring a Remote MEP with an Iterator Profile | 270

Use this topic to configure an iterator profile that periodically transmits SLA measurement packets for delay and loss measurement. You can also view and clear the iterator statistics, and configure a remote MEP with an iterator profile.

Configuring an Iterator Profile

You can create an iterator profile with its parameters to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for delay measurement or loss measurement.

To create an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure the SLA measurement monitoring iterator:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# edit sla-iterator-profiles
```

3. Configure an iterator profile—for example, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# set i1
```

4. (Optional) Configure the cycle time, which is the amount of time (in milliseconds) between back-to-back transmission of SLA frames for one connection, with values from 10 through 3,600,000. The default value is 1000 ms.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set cycle-time cycle-time-value
```

5. (Optional) Configure the iteration period, which indicates the maximum number of cycles per iteration (the number of connections registered to an iterator cannot exceed this value), with values from 1 through 2000. The default value is 2000.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set iteration-period iteration-period-value
```

6. Configure the measurement type as loss measurement, statistical frame-loss measurement, or two-way delay measurement.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set measurement-type (loss | statistical-frame-loss | two-way-delay)
```

7. (Optional) Configure the calculation weight for delay with values from 1 through 65,535. The default value is 1 (applicable only for two-way delay measurement).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set calculation-weight delay delay-value
```

8. (Optional) Configure the calculation weight for delay variation with values from 1 through 65,535. The default value is 1 (applicable only for two-way delay measurement).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set calculation-weight delay-variation delay-variation-value
```

9. (Optional) Configure the threshold value for average frame delay, in microseconds, for two-way Ethernet frame delay measurement (ETH-DM). When the configured threshold for average frame delay is exceeded, an SNMP trap is generated for ETH-DM. The range is from 1 through 4294967295 microseconds.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set avg-fd-twoway-threshold avg-fd-twoway-threshold-value
```

10. (Optional) Configure the threshold value for average frame delay variation, in microseconds, for two-way Ethernet frame delay measurement (ETH-DM). When the configured threshold for average frame delay variationis exceeded, an SNMP trap is generated for ETH-DM. The range is from 1 through 4294967295 microseconds.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set avg-ifdv-twoway-threshold avg-ifdv-twoway-threshold-value
```

11. (Optional) Configure the threshold value for average frame loss ratio, in milli-percent, in the upward or forward direction for Ethernet loss measurement (ETH-LM) and Ethernet synthetic loss measurement (ETH-SLM). When the configured threshold for average forward frame loss ratio is exceeded, an SNMP trap is generated for ETH-LM and ETH-SLM. The range is from 1 through 100000 milli-percent.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set avg-flr-forward-threshold avg-flr-forward-threshold-value
```

12. (Optional) Configure the threshold value for average frame loss ratio, in milli-percent, in the backward or downstream direction for Ethernet loss measurement (ETH-LM) and Ethernet synthetic loss measurement (ETH-SLM). When the configured threshold for average backward frame loss ratio is exceeded, an SNMP trap is generated for ETH-LM and ETH-SLM. The range is from 1 through 100000 milli-percent.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set avg-flr-backward-threshold avg-flr-backward-threshold-value
```

13. Configure the **disable** statement to stop the iterator (that is, disable the iterator profile).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set disable
```

14. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# show i1
  cycle-time cycle-time-value;
  iteration-period iteration-period-value;
  measurement-type (loss | two-way-delay);
  avg-fd-twoway-threshold avg-fd-twoway-threshold-value;
  avg-ifdv-twoway-threshold avg-ifdv-twoway-threshold-value;
  avg-flr-forward-threshold avg-flr-forward-threshold-value;
  avg-flr-backward-threshold avg-flr-backward-threshold-value;
  calculation-weight {
    delay delay-weight;
    delay-variation delay-variation-weight;
  }
  calculation-weight {
```

```
    delay delay-weight;
    delay-variation delay-variation-weight;
}
```

SEE ALSO

- Proactive Mode for SLA Measurement | **176**

Verifying the Configuration of an Iterator Profile

IN THIS SECTION

- Displaying the Configuration of an Iterator Profile for Two-way Delay Measurement | **261**
- Displaying the Configuration of an Iterator Profile for Loss Measurement | **262**
- Displaying the Configuration of a Remote MEP with an Iterator Profile | **263**
- Disabling an Iterator Profile | **263**

The following topics illustrate the configuration of an iterator profile for a two-way delay measurement, for loss measurement, and for a remote maintenance association end point (MEP). The topics also illustrate disabling an iterator profile with the **disable** statement for two-way measurement and deactivating an iterator profile with the **deactivate** command for a remote MEP.

Displaying the Configuration of an Iterator Profile for Two-way Delay Measurement

Purpose

Display the configuration of an iterator profile for two-way delay measurement as configured in the "Configuring an Iterator Profile" on page 258 topic with the following values:

- **profile-name**—**i1**
- **cycle-time**—**1000** milliseconds
- **iteration-period**—**2000** cycles per second
- **delay**—**1**
- **delay-variation**—**1**:

Action

To display information about the iterator profile, run the **show** command at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# show
i1 {
    cycle-time 1000;
    iteration-period 2000;
    measurement-type two-way-delay;
    calculation-weight {
        delay 1;
        delay-variation 1;
    }
}
```

Meaning

The configuration for an iterator profile for two-way measurement is displayed as expected with set values.

Displaying the Configuration of an Iterator Profile for Loss Measurement

Purpose

Display the configuration of an iterator profile for loss measurement as configured in the "Configuring an Iterator Profile" on page 258 topic with the following values:

- **profile-name**—**12**
- **cycle-time**—**1000** milliseconds
- **iteration-period**—**2000** cycles per second

Action

To display information about the iterator profile, run the **show** command at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# show
12 {
    cycle-time 1000;
    iteration-period 2000;
    measurement-type loss;
}
```

Meaning

The configuration for an iterator profile for loss measurement is displayed as expected with set values.

Displaying the Configuration of a Remote MEP with an Iterator Profile

Purpose

Display the configuration of a remoteMEP as configured in the "Configuring a Remote MEP with an Iterator Profile" on page 270 topic with the following values:

- **profile-name—i3**
- **maintenance-domain—default-1**
- **maintenance-association—1**
- **short-name-format—2octet**
- **mep—1**
- **remote-mep—1**
- **data-tlv-size—1**
- **iteration-count—1**
- **priority—1**

Action

To display information about the remote MEP, run the **show** command at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance association ma1 mep 1 remote-mep 1]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance
   association 1 short-name-format 2octet mep 1 remote-mep 1]
user@host# show
sla-iterator-profile i3 {
   data-tlv-size 1;
   iteration-count 1;
   priority 1;
}
```

Meaning

The configuration for a remote MEP for two-way measurement is displayed as expected with set values.

Disabling an Iterator Profile

Purpose

To disable an iterator profile for two-way delay measurement and for a remote MEP.

Action

- To disable an iterator profile (for example, i1) with the **disable** configuration command for two-way measurement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles i1]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles i1]
user@host# disable
```

- To disable an iterator profile for a remote MEP (for example, i2) with the **deactivate** configuration command at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance association ma1 mep 1 remote-mep 1]** hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance
    association ma1 mep 1 remote-mep 1]
user@host# deactivate sla-iterator-profile i2
```

SEE ALSO

Proactive Mode for SLA Measurement | 176

Managing Iterator Statistics

IN THIS SECTION

Displaying Iterator Statistics | 264
Clearing Iterator Statistics | 270

Displaying Iterator Statistics

Purpose

Retrieve and display iterator statistics.

Muliple iterators can be associated with a remote MEP. However, by default, only one result pertaining to one iterator profile is displayed.

Action

- To display the iterator statistics for remote MEP **1** and iterator profile **i1** with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1** (here, the iterator profile **i1** is configured for two-way delay measurement):

user@host> **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1**

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i1, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap

Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent                                        : 23898520
DMM skipped for threshold hit                   : 11000
DMM skipped for threshold hit window            : 0
DMR received                                    : 23851165
DMR out of sequence                             : 1142
DMR received with invalid time stamps           : 36540
Average two-way delay                           : 129 usec
Average two-way delay variation                 : 15 usec
Average one-way forward delay variation         : 22 usec
Average one-way backward delay variation        : 22 usec
Weighted average two-way delay                  : 134 usec
Weighted average two-way delay variation        : 8 usec
Weighted average one-way forward delay variation  : 6 usec
Weighted average one-way backward delay variation : 2 usec
```

Output fields are listed in the approximate order in which they appear.

Table 19: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields

Output Field Name	Output Field Description
Maintenance domain	Maintenance domain name.
Level	Maintenance domain level configured.
Maintenance association	Maintenance association name.
Local MEP id	Numeric identifier of the local MEP.
Remote MEP id	Numeric identifier of the remote MEP.

Table 19: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields *(continued)*

Output Field Name	Output Field Description
Remote MAC address	Unicast MAC address of the remote MEP.
Iterator name	Name of iterator.
Iterator Id	Numeric identifier of the iterator.
Iterator cycle time	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
Iteration period	Maximum number of cycles per iteration
Iterator status	Current status of iterator whether running or stopped.
Infinite iterations	Status of iteration as infinite or finite.
Counter reset time	Date and time when the counter was reset.
Reset reason	Reason to reset counter.
Delay weight	Calculation weight of delay.
Delay variation weight	Calculation weight of delay variation.
DMM sent	Delay measurement message (DMM) PDU frames sent to the peer MEP in this session.
DMM skipped for threshold hit	Number of DMM frames sent to the peer MEP in this session skipped during threshold hit.
DMM skipped for threshold hit window	Number of DMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
DMR received	Number of delay measurement reply (DMR) frames received.
DMR out of sequence	Total number of DMR out of sequence packets received.
DMR received with invalid time stamps	Total number of DMR frames received with invalid timestamps.
Average two-way delay	Average two-way frame delay for the statistics displayed.

Table 19: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields *(continued)*

Output Field Name	Output Field Description
Average two-way delay variation	Average two-way “frame jitter” for the statistics displayed.
Average one-way forward delay variation	Average one-way forward delay variation for the statistics displayed in microseconds.
Average one-way backward delay variation	Average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average two-way delay	Weighted average two-way delay for the statistics displayed in microseconds.
Weighted average two-way delay variation	Weighted average two-way delay variation for the statistics displayed in microseconds.
Weighted average one-way forward delay variation	Weighted average one-way forward delay variation for the statistics displayed in microseconds.
Weighted average one-way backward delay variation	Weighted average one-way backward delay variation for the statistics displayed in microseconds.

- To display the iterator statistics for remote MEP **1** and iterator profile **i2** with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1** (here, the iterator profile **i1** is configured for loss measurement):

  `user@host>` **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1**

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i2, Iterator Id: 2
Iterator cycle time: 1000ms, Iteration period: 2000 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:25 ago)
Reset reason: Adjacency flap

Iterator loss measurement statistics:
```

```
LMM sent                              : 238970
LMM skipped for threshold hit         : 60
LMM skipped for threshold hit window  : 0
LMR received                          : 238766
LMR out of sequence                   : 43

Accumulated transmit statistics:
Near-end (CIR)                        : 0
Far-end (CIR)                         : 0
Near-end (EIR)                        : 0
Far-end (EIR)                         : 0

Accumulated loss statistics:
Near-end (CIR)                        : 0 (0.00%)
Far-end (CIR)                         : 0 (0.00%)
Near-end (EIR)                        : 0 (0.00%)
Far-end (EIR)                         : 0 (0.00%)

Last loss measurement statistics:
Near-end (CIR)                        : 0
Far-end (CIR)                         : 0
Near-end (EIR)                        : 0
Far-end (EIR)                         : 0
```

Output fields are listed in the approximate order in which they appear.

Table 20: Displaying Iterator Statistics for Ethernet Loss Measurement Output Fields

Output Field Name	Output Field Description
Maintenance domain	Maintenance domain name.
Level	Maintenance domain level configured.
Maintenance association	Maintenance association name.
Local MEP id	Numeric identifier of the local MEP.
RemoteMEP identifier	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Iterator name	Name of iterator.
Iterator Id	Numeric identifier of the iterator.

Table 20: Displaying Iterator Statistics for Ethernet Loss Measurement Output Fields *(continued)*

Output Field Name	Output Field Description
Iterator cycle time	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
Iteration period	Maximum number of cycles per iteration
Iterator status	Current status of iterator whether running or stopped.
Infinite iterations	Status of iteration as infinite or finite.
Counter reset time	Date and time when the counter was reset.
Reset reason	Reason to reset counter.
LMM sent	Number of loss measurement message (LMM) PDU frames sent to the peer MEP in this session.
LMM skipped for threshold hit	Number of LMM frames sent to the peer MEP in this session skipped during threshold hit.
LMM skipped for threshold hit window	Number of LMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
LMR received	Number of LMRs frames received.
LMR out of sequence	Total number of LMR out of sequence packets received.
Near-end (CIR)	Frame loss associated with ingress data frames for the statistics displayed.
Far-end (CIR)	Frame loss associated with egress data frames for the statistics displayed.
Near-end (EIR)	Frame loss associated with ingress data frames for the statistics displayed.
Far-end (EIR)	Frame loss associated with egress data frames for the statistics displayed.

SEE ALSO

Proactive Mode for SLA Measurement | **176**

show oam ethernet connectivity-fault-management sla-iterator-statistics | **2714**

clear oam ethernet connectivity-fault-management sla-iterator-statistics | 2636

Clearing Iterator Statistics

Purpose

Clear iterator statistics.

Multiple iterators can be associated with remote MEP. However, by default, only one result pertaining to one iterator profile can be cleared.

Action

- To clear the iterator statistics for remote MEP **1** and iterator profile **i1** with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1**:

  ```
  user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i1
  maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
  ```

- To clear the iterator statistics for remote MEP **1** and iterator profile **i2** with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1**:

  ```
  user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i2
  maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
  ```

SEE ALSO

Proactive Mode for SLA Measurement | 176

show oam ethernet connectivity-fault-management sla-iterator-statistics | 2714

clear oam ethernet connectivity-fault-management sla-iterator-statistics | 2636

SEE ALSO

Proactive Mode for SLA Measurement | 176

Configuring a Remote MEP with an Iterator Profile

You can associate a remote maintenance association end point (MEP) with more than one iterator profile.

To configure a remote MEP with an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id
```

2. Configure the remote MEP with values from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id]
user@host# set remote-mep remote-mep-id
```

3. Set the iterator profile.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# set sla-iterator-profile profile-name
```

4. (Optional) Set the size of the data TLV portion of the Y.1731 data frame with values from 1 through 1400 bytes. The default value is 1.

```
[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]
user@host# set data-tlv-size size
```

5. (Optional) Set the iteration count, which indicates the number of iterations for which this connection should partake in the iterator for acquiring SLA measurements, with values from 1 through 65,535. The default value is 0 (that is, infinite iterations).

```
[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]
user@host# set iteration-count count-value
```

6. (Optional) Set the priority, which is the **vlan-pcp** value that is sent in the Y.1731 data frames, with values from 0 through 7. The default value is 0.

```
[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]
user@host# set priority priority-value
```

7. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# show
sla-iterator-profile profile-name {
   data-tlv-size size;
   iteration-count count-value;
   priority priority-value;
}
```

SEE ALSO

- Proactive Mode for SLA Measurement | 176
- remote-mep | 1842

RELATED DOCUMENTATION

- ITU-T Y.1731 Ethernet Service OAM Overview | 165
- Configuring Ethernet Frame Delay Measurement Sessions | 185

Configuring Ethernet Synthetic Loss Measurements

IN THIS SECTION

- Guidelines for Configuring ETH-SLM | 273
- Starting a Proactive ETH-SLM Session | 274
- Starting an On-Demand ETH-SLM Session | 279
- Managing ETH-SLM Statistics and ETH-SLM Frame Counts | 280
- Troubleshooting Failures with ETH-SLM | 285

Use this topic to understand the guidelines for configuring synthetic loss measurement and how to start a synthetic loss measurement session. There are two types of synthetic loss measurement sessions: proactive and On-Demand. This topic describes both. Also, the topic shows you how to view and clear the synthetic loss measurement statistics and how to troubleshoot failures with SLM.

Guidelines for Configuring ETH-SLM

Keep the following points in mind when you configure the ETH-SLM functionality:

- The monitoring application for Ethernet OAM is initiated in the master Routing Engine. When a stateful switchover process occurs, the monitoring application is disabled. For on-demand ETH-SLM, graceful Routing Engine switchover (GRES) support is not applicable. For proactive ETH-SLM, the service-level agreement (SLA) iterators are restored during a stateful switchover process. If the adjacencies do not time out, the ETH-SLM statistics are preserved and proactive ETH-SLM supports GRES.
- ETH-SLM is initiated only when the MEP session is up. Unified in-service software upgrade (ISSU) support for ETH-SLM depends on the unified ISSU support for CFM. For CFM, unified ISSU is supported using the loss threshold TLV to avoid CFM connectivity loss during the upgrade. The receiving or the destination MEP increases the threshold time during the termination of sessions. If you start a unified ISSU operation when on-demand ETH-SLM is in progress, the SLM request and reply messages are lost at the local Packet Forwarding Engine.

  When an on-demand ETH-SLM is requested, if the local source MEP undergoes a unified ISSU, a message is displayed stating that the MEP is undergoing a unified ISSU. If the remote MEP is undergoing a unified ISSU (detected through the loss threshold TLV), a message is displayed stating that the remote MEP is undergoing a unified ISSU. Also, if it is not possible to identify whether unified ISSU is in progress on a remote MEP, the SLM packets are lost at the system where unified ISSU is in progress and the loss calculation results do not provide a valid cause for the loss. Unified ISSU is not supported for both on-demand and proactive ETH-SLM.
- The maximum number of SLA iterator profiles that can be configured in the system is 255.
- ETH-SLM is not supported for virtual private LAN service (VPLS) (point-to-multipoint measurements are not supported). The ETH-SLM frames are not generated with multicast class 1 destination address. Similarly, ETH-SLM does not respond to ETH-SLM requests with multicast DA. ETH-SLM for VPLS for point-to-point Ethernet connection is supported using directed unicast destination MAC addresses, although point-to-multipoint topologies are not supported.
- A unicast destination address may be used in provisioned environments for point-to-point connections. However, it requires that the unicast destination address of the downstream MEP must have been configured on the MEP transmitting an alarm indication signal (AIS).
- ETH-SLM is not supported on downstream MEPs on label-switched interfaces (LSIs).
- ETH-SLM is supported on aggregated Ethernet (ae) interfaces
- The number of ETH-SLM sessions for proactive ETH-SLM that can be supported is limited to the total number of iterators that can be supported in the system. This limitation includes the iterator support for other measurement types such as loss, statistical frame loss, and two-way delay. A new iterator type, SLM, is added to support ETH-SLM. The total number of SLA iterators that you can configure in the system is equal to the total number of iterations supported in the system.
- For on-demand SLM, the minimum period between two SLM requests is 100 milliseconds.

- For proactive SLM, the minimum period between two SLM requests is 10 milliseconds for distributed mode and 100 milliseconds for non-distributed mode.
- ETH-SLM frames are always marked as drop-ineligible in compliance with the ITU-T Y.1731 standard.

SEE ALSO

Ethernet Synthetic Loss Measurement Overview | 178

monitor ethernet synthetic-loss-measurement | 2669

Starting a Proactive ETH-SLM Session

IN THIS SECTION

- Configuring MEP Interfaces | 274
- Configuring an Iterator Profile for ETH-SLM | 275
- Associating the Iterator Profile with MEPs for ETH-SLM | 277

To start a proactive Ethernet synthetic loss measurement (ETH-SLM) session, you must configure the Ethernet interfaces on maintenance association end points (MEPs) on which packets transmitted with synthetic frame loss need to be analyzed. You must then create an iterator profile to transmit service-level agreement (SLA) measurement packets for ETH-SLM and associate the local and remote MEPs with the profile.

Configuring MEP Interfaces

Before you can start an Ethernet synthetic frame loss measurement session across an Ethernet service, you must configure two ACX Series routers to support ETH-SLM.

To configure an Ethernet interface on an ACX Series router to support ETH-SLM:

1. On each router, configure two physical or logical Ethernet interfaces connected by a VLAN. The following configuration is typical for single-tagged logical interfaces:

```
[edit interfaces]
interface {
    ethernet-interface-name {
        vlan-tagging;
        unit logical-unit-number {
```

```
            vlan-id vlan-id; # Both interfaces on this VLAN
        }
    }
}
```

Both interfaces will use the same VLAN ID.

2. On each router, attach peer MEPs to the two interfaces. The following configuration is typical:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md-name { # On both routers
                level number;
                maintenance-association ma-name { # On both routers
                    continuity-check {
                        interval 100ms;
                        hold-interval 1;
                    }
                    mep mep-id { # Attach to VLAN interface
                        auto-discovery;
                        direction (up | down);
                        interface interface-name;
                        priority number;
                    }
                }
            }
        }
    }
}
```

Configuring an Iterator Profile for ETH-SLM

You can create an iterator profile with its parameters to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for synthetic loss measurement.

NOTE: ACX5048 and ACX5096 routers supports iterator cycle time of only 1 second and above.

To create an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure the SLA measurement monitoring iterator:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# edit sla-iterator-profiles
```

3. Configure an iterator profile—for example, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# set i1
```

4. (Optional) Configure the cycle time, which is the amount of time (in milliseconds) between back-to-back transmission of SLA frames for one connection, with a value from 10 through 3,600,000. The default value is 1000 ms.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set cycle-time cycle-time-value
```

5. (Optional) Configure the iteration period, which indicates the maximum number of cycles per iteration (the number of connections registered to an iterator cannot exceed this value), with a value from 1 through 2000. The default value is 2000.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set iteration-period iteration-period-value
```

6. Configure the measurement type as synthetic loss measurement.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@host# set measurement-type slm
```

7. Configure the **disable** statement to stop the iterator (that is, disable the iterator profile).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    i1]
user@host# set disable
```

8. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
user@host# show i1
    cycle-time cycle-time-value;
    iteration-period iteration-period-value;
    measurement-type slm;
```

Associating the Iterator Profile with MEPs for ETH-SLM

You can associate a remote maintenance association end point (MEP) with more than one iterator profile.

To configure a remote MEP with an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id
```

2. Configure the remote MEP ID with a value from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id]
user@host# set remote-mep remote-mep-id
```

3. Set the iterator profile.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
    maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# set sla-iterator-profile profile-name
```

4. (Optional) Set the size of the data TLV portion of the Y.1731 data frame with a value from 1 through 1400 bytes. The default value is 1.

```
[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]
```

```
user@host# set data-tlv-size size
```

5. (Optional) Set the iteration count, which indicates the number of iterations for which this connection should partake in the iterator for acquiring SLA measurements, with a value from 1 through 65,535. The default value is 0 (that is, infinite iterations).

```
[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]
user@host# set iteration-count count-value
```

6. (Optional) Set the priority, which is the **vlan-pcp** value that is sent in the Y.1731 data frames, with a value from 0 through 7. The default value is 0.

```
[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]
user@host# set priority priority-value
```

7. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# show
sla-iterator-profile profile-name  {
   data-tlv-size size;
   iteration-count count-value;
   priority priority-value;
}
```

SEE ALSO

Ethernet Synthetic Loss Measurement Overview | 178

monitor ethernet synthetic-loss-measurement | 2669

Starting an On-Demand ETH-SLM Session

To start an on-demand Ethernet synthetic loss measurement (ETH-SLM) session, type the **monitor ethernet synthetic-loss-measurement one-way** command in operational mode, and specify the peer MEP by its MAC address or by its MEP identifier.

For example:

```
user@host> monitor ethernet synthetic-loss-measurement 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
```

```
ETH-SLM request to 00:05:85:73:39:4a, interface ge-1/0/0.0
      Synthetic Loss measurement statistics:
       SLM packets sent                          : 100
       SLR packets received                      : 100
       Accumulated SLM statistics:
       Local TXFC1 value                         : 100
       Local RXFC1 value                         : 100
       Last Received SLR frame TXFCf(tc)         : 100
       Last Received SLR frame TXFCb(tc)         : 100
       SLM Frame Loss:
       Frame Loss (far-end)                      : 0 (0.00 %)
       Frame Loss (near-end)                     : 0 (0.00 %)
```

NOTE: If you attempt to monitor delays to a nonexistent MAC address, you must press **Ctrl + C** to explicitly quit the **monitor ethernet synthetic-loss-measurement** command and return to the CLI command prompt.

SEE ALSO

Ethernet Synthetic Loss Measurement Overview | 178

monitor ethernet synthetic-loss-measurement | 2669

Managing ETH-SLM Statistics and ETH-SLM Frame Counts

IN THIS SECTION

- Displaying ETH-SLM Statistics Only | **280**
- Displaying ETH-SLM Statistics and Frame Counts | **281**
- Displaying ETH-SLM Frame Counts for MEPs by Enclosing CFM Entity | **282**
- Displaying ETH-SLM Frame Counts for MEPs by Interface or Domain Level | **283**
- Clearing ETH-SLM Statistics and Frame Counts | **284**
- Clearing Iterator Statistics | **284**

Displaying ETH-SLM Statistics Only

Purpose

Display on-demand ETH-SLM statistics.

By default, the **show oam ethernet connectivity-fault-management synthetic-loss-statistics** command displays on-demand ETH-SLM statistics for MEPs in the specified CFM maintenance association within the specified CFM maintenance domain.

Action

- To display the on-demand ETH-SLM statistics collected for MEPs belonging to maintenance association **ma1** within maintenance domain **md1**:

  ```
  user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
  maintenance-domain md1 maintenance-association ma1
  ```

- To display the on-demand ETH-SLM statistics collected for ETH-SLM sessions for the local MEP **201** belonging to maintenance association **ma2** within maintenance domain **md2**:

  ```
  user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
  maintenance-domain md2 maintenance-association ma2 local-mep 201
  ```

- To display the on-demand ETH-SLM statistics collected for ETH-SLM sessions from local MEPs belonging to maintenance association **ma3** within maintenance domain **md3** to the remote MEP **302**:

  ```
  user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
  maintenance-domain md3 maintenance-association ma3 remote-mep 302
  ```

Meaning

The output displays on-demand ETH-SLM statistics for MEPs in the specified maintenance association within the specified maintenance domain. For details about the output of this command and the descriptions of the output fields, see **show oam ethernet connectivity-fault-management synthetic-loss-statistics**.

SEE ALSO

show oam ethernet connectivity-fault-management synthetic-loss-statistics

Displaying ETH-SLM Statistics and Frame Counts

Purpose

Display on-demand ETH-SLM statistics and ETH-SLM frame counts.

By default, the **show oam ethernet connectivity-fault-management mep-statistics** command displays on-demand ETH-SLM statistics and frame counts for MEPs in the specified CFM maintenance association within the specified CFM maintenance domain.

Action

- To display the on-demand ETH-SLM statistics and ETH-SLM frame counts for MEPs in maintenance association **ma1** within maintenance domain **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma1**

- To display the on-demand ETH-SLM statistics and ETH-SLM frame counts for the local MEP **201** in maintenance association **ma2** within maintenance domain **md2**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md2 maintenance-association ma2 local-mep 201**

- To display the on-demand ETH-SLM statistics and ETH-SLM frame counts for the local MEP in maintenance association **ma3** within maintenance domain **md3** that participates in an ETH-SLM session with the remote MEP **302**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain ma3 maintenance-association ma3 remote-mep 302**

Meaning

The output displays on-demand ETH-SLM statistics and ETH-SLM frame counts for MEPs in the specified maintenance association within the specified maintenance domain. For details about the output of this command and the descriptions of the output fields, see **show oam ethernet connectivity-fault-management mep-statistics**.

SEE ALSO

show oam ethernet connectivity-fault-management mep-statistics

Displaying ETH-SLM Frame Counts for MEPs by Enclosing CFM Entity

Purpose

Display on-demand ETH-SLM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management mep-database** command displays CFM database information for MEPs in the specified CFM maintenance association within the specified CFM maintenance domain.

> **NOTE:** At the router attached to the initiator MEP for a one-way session, or at the router attached to the receiver MEP for a two-way session, you can only display the ETH-SLM frame counts and not the MEP database details.

Action

- To display CFM database information (including ETH-SLM frame counts) for all MEPs in MA **ma1** within maintenance domain **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain ma1 maintenance-association ma1**

- To display CFM database information (including ETH-SLM frame counts) only for the local MEP **201** in MA **ma1** within maintenance domain **md1**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md2 maintenance-association ma2 local-mep 201**

- To display CFM database information (including ETH-SLM frame counts) only for the remote MEP **302** in MA **ma3** within maintenance domain **md3**:

  `user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain ma3 maintenance-association ma3 remote-mep 302**

Meaning

The output displays ETH-SLM frame counts for MEPs within a particular maintenance domain, or for a specific local or remote MEP. For details about the output of this command and the descriptions of the output fields, see **show oam ethernet connectivity-fault-management mep-database**.

SEE ALSO

show oam ethernet connectivity-fault-management mep-database

Displaying ETH-SLM Frame Counts for MEPs by Interface or Domain Level

Purpose

Display on-demand ETH-SLM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management interfaces** command displays CFM database information for MEPs attached to CFM-enabled Ethernet interfaces on the router or at a maintenance domain level. For Ethernet interfaces that support ETH-SLM, any frame counts are also displayed when you specify the **detail** or **extensive** command option.

NOTE: At the router attached to the initiator MEP, you can only display the ETH-SLM frame counts and not the MEP database details.

Action

- To display CFM database information (including ETH-SLM frame counts) for all MEPs attached to CFM-enabled Ethernet interfaces on the router:

  `user@host>` **show oam ethernet connectivity-fault-management interfaces detail**

- To display CFM database information (including ETH-SLM frame counts) only for the MEPs attached to CFM-enabled router interface **ge-5/2/9.0**:

  `user@host>` **show oam ethernet connectivity-fault-management interfaces ge-5/2/9.0 detail**

- To display CFM database information (including ETH-SLM frame counts) only for MEPs enclosed within CFM maintenance domains at level ***6***:

  `user@host>` **show oam ethernet connectivity-fault-management interfaces level 6 detail**

Meaning

The output displays ETH-SLM frame counts for MEPs for the specified interface. For details about the output of this command and the descriptions of the output fields, see **show oam ethernet connectivity-fault-management interfaces**.

SEE ALSO

show oam ethernet connectivity-fault-management interfaces

Clearing ETH-SLM Statistics and Frame Counts

Purpose

Clear the on-demand ETH-SLM statistics and ETH-SLM frame counts.

By default, statistics and frame counts are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

Action

- To clear the on-demand ETH-SLM statistics and ETH-SLM frame counts for all MEPs attached to CFM-enabled interfaces on the router:

  `user@host>` **clear oam ethernet connectivity-fault-management synthetic-loss-measurement**

- To clear the on-demand ETH-SLM statistics and ETH-SLM frame counts only for MEPs attached to the logical interface **ge-0/5.9.0**:

  `user@host>` **clear oam ethernet connectivity-fault-management synthetic-loss-measurement ge-0/5/9.0**

Clearing Iterator Statistics

Purpose

Clear the existing iterator statistics and proactive ETH-SLM counters.

Multiple iterators can be associated with remote MEP. However, by default, only one result pertaining to one iterator profile can be cleared.

Action

- To clear the iterator statistics for remote MEP **1** and iterator profile **i1** with MEPs belonging to the maintenance association **ma1** within the maintenance domain **default-1**:

  `user@host>` **clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep *1***

- To clear the iterator statistics for remote MEP **1** and iterator profile **i2** with MEPs belonging to the maintenance association **ma1** within the maintenance domain **default-1**:

  `user@host>` **clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1**

SEE ALSO

clear oam ethernet connectivity-fault-management synthetic-loss-measurement | 2649

show oam ethernet connectivity-fault-management synthetic-loss-statistics | 2799

show oam ethernet connectivity-fault-management interfaces | 2727 (**detail** | **extensive**)

show oam ethernet connectivity-fault-management mep-statistics | 2764

show oam ethernet connectivity-fault-management mep-database | 2749

Troubleshooting Failures with ETH-SLM

Problem

Description: The Ethernet synthetic loss measurement (ETH-SLM) application is not working properly for calculation of frame loss using synthetic frames instead of data traffic

Solution

Perform the following steps to analyze and debug any problems with the ETH-SLM functionality.

1. Ensure that ETH-SLM is configured (either proactive or on-demand) to initiate SLM frames. Verify the configuration settings.

2. Examine any failures that might have occurred in the CFM session for which the ETH-SLM feature is enabled. The CFM session must be in the up state for the ETH-SLM functionality to work correctly. Use the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *md-name* maintenance-association *ma-name* local-mep *mep-id* remote-mep *remote-mep-id*** command to verify whether the CFM session is in the up state.

3. If the MEP sessions are active, use the appropriate show command to verify the ETH-SLM statistics and to analyze if ETH-SLM frames are transmitted or received.

4. If the transmission of ETH-SLM frames does not happen correctly after you attempt all of the preceding troubleshooting steps, enable the tracing operations for Ethernet CFM by including the **traceoptions** statement at the [**edit protocols oam ethernet connectivity-fault-management**] hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management]
traceoptions {
   file <filename> <files number  <match regular-expression microsecond-stamp>> <size size> <world-readable |
      no-world-readable>;
   flag flag;
   no-remote-trace;
}
```

SEE ALSO

Ethernet Synthetic Loss Measurement Overview | 178
monitor ethernet synthetic-loss-measurement | 2669

RELATED DOCUMENTATION

ITU-T Y.1731 Ethernet Service OAM Overview | 165
Configuring Ethernet Frame Loss Measurement | 223

Ethernet Alarm Indication

IN THIS SECTION

- Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286
- Ethernet Alarm Indication Signal Overview | 291
- Configuring ETH-AIS on a CFM MEP | 292
- Configuring Alarm Indication Signal on ACX Series Routers | 297

Use the following to understand more about Ethernet alarm indication signal (ETH-AIS) and how to configure ETH-AIS on devices.

Ethernet Alarm Indication Signal (ETH-AIS) Function Overview

IN THIS SECTION

- Understanding ETH-AIS in a Maintenance Domain | 287
- Fault Detection in a Maintenance Domain | 287
- Terms Defined | 289

Ethernet alarm indication signal (ETH-AIS) function enables a service provider deploying an Ethernet service to determine whether a connectivity fault exists at the provider's domain level or at a level below. When the fault occurs at the provider's domain level, the service provider addresses the fault, and when the fault occurs at a level below, the provider can either ignore the fault or contact the relevant authorities to address the fault.

The following sections explain ETH-AIS, few use cases which determine when to generate and propagate ETH-AIS packets, and associated terms in detail:

Understanding ETH-AIS in a Maintenance Domain

ITU-T developed Y.1731 as a recommendation for Operation, Administration, and Maintenance (OAM) functions and mechanisms for Ethernet-based networks, including OAM functions such as ETH-AIS, Ethernet locked signal (ETH-LCK), Ethernet test signal (ETH-Test), Ethernet automatic protection switching (ETH-APS), Ethernet maintenance communication channel (ETH-MCC), Ethernet experimental OAM (ETH-EXP), Ethernet vendor-specific OAM (ETH-VSP), and performance monitoring. For information about maintenance domain and related terms, see "Terms Defined" on page 289.

According to the Y.1731 standards, a server MEP is a combined function of the server layer termination function and the server Ethernet services layer adaptation function. The server MEP notifies the Ethernet services (ETH) layer MEPs when it detects a failure. The server layer termination function then runs the OAM mechanisms specific to the server layer and the alarms are suppressed at the server layer by ETH-AIS.

Note that ETH-AIS is not applicable to Spanning Tree Protocol (STP) networks.

ETH-AIS enables you to suppress alarms when a fault condition is detected. Using ETH-AIS, a service provider can differentiate between faults at different levels.

ETH-AIS provides many advantages that include:

- Service providers need not raise alarms if there are lower-level failures.
- Service providers can provide a refund to their subscribers or avail a refund from their Internet provider based on service unavailability.

MX Series routers support ITU-T Y.1731 ETH-AIS to provide fault management for service providers who provide carrier Ethernet services using IEEE 802.1ag standard.

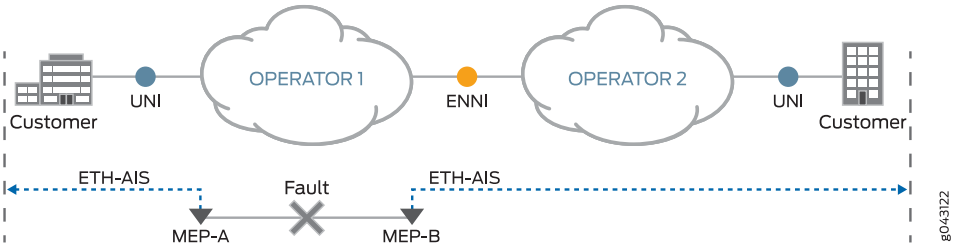
> **NOTE:** MX Series Virtual Chassis does not support Ethernet alarm indication signal (ETH-AIS).

Fault Detection in a Maintenance Domain

In the scenario depicted in Figure 1 on page xyz, you have a service provider level and a customer level. Two service providers—*Operator-1* and *Operator-2*—are considered for illustration purposes. Assume that a fault occurs in Operator-1 maintenance domain-level that has MEP-A and MEP-B at its maintenance domain-level boundaries. To notify the faults to a network management system and to avoid notification

of alarms from the customer level for the same fault, MEP-A and MEP-B transmit an alarm indication signal (AIS) on opposite directions, thereby signaling the higher levels and the Operator-2 network about the fault, so that the alarms are suppressed.

Signaling is achieved through transmission and propagation of AIS protocol data units (PDUs). You must enable AIS explicitly on all the MEPs at the service provider level. A MEP that is configured to issue frames with ETH-AIS information is generally at the server layer and continues to transmit periodic frames with ETH-AIS information until the defect condition is cleared. When a client MEP receives the ETH-AIS frames, it suppresses loss-of-continuity alarms associated with its peer MEPs.



Note that in the absence of AIS, a client MEP resumes generating loss-of-continuity alarms when it detects the loss-of-continuity defect conditions from its server layer.

For point-to-point Ethernet services layer connectivity, a MEP has only one peer MEP. Therefore, there is no ambiguity regarding the peer MEP for which the MEP should suppress alarms when it receives the ETH-AIS information.

For multipoint Ethernet services layer connectivity, a MEP that receives ETH-AIS information cannot determine the exact MEP that encountered the fault and, therefore, cannot isolate the exact peer MEP to suppress the alarms. To avoid this scenario, Y.1731 recommends suppressing alarms for all peer MEPs in the same domain level irrespective of connectivity status in a multipoint Ethernet services layer connectivity setup.

Table 21 on page 288 lists the operational mode commands that you can use in a maintenance domain to check the various parameters pertaining to a MEP.

Table 21: Operational Mode Commands

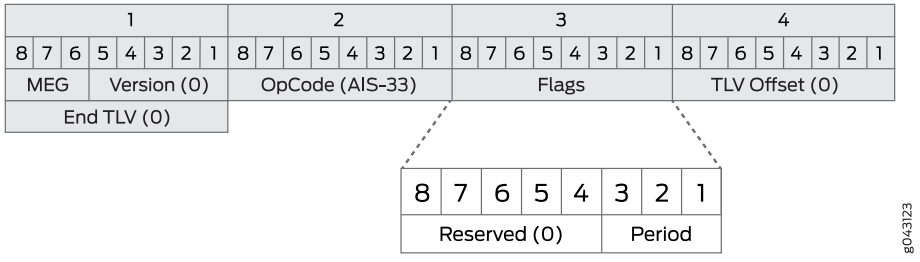
To Check	Operational Mode Commands
Whether the AIS configuration is configured correctly on a CFM MEP.	**show protocols oam ethernet connectivity-fault-management action-profile**

Table 21: Operational Mode Commands *(continued)*

To Check	Operational Mode Commands
Statistics of AIS frames.	**show oam ethernet connectivity-fault-management interfaces detail** **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain *md-name* maintenance-association *ma-name* remote-mep *mep-id* local-mep *mep-id***
Whether any event has occurred that triggered AIS.	**show oam ethernet connectivity-fault-management mep-database maintenance-domain *md-name* maintenance-association *ma-name* remote-mep *mep-id* local-mep *mep-id***
Status of CFM sessions for faults that trigger AIS on the MEP.	**show oam ethernet connectivity-fault-management interfaces detail**

Terms Defined

- AIS transmission—A MEP upon detecting a defect condition transmits AIS frames in a direction opposite to its peer MEPs. The periodicity of AIS frames transmission is on the basis of the AIS transmission period. An AIS transmission period of 1 second is recommended. The first AIS frame must always be transmitted immediately following the detection of a defect condition.
- AIS reception—Upon receiving an AIS frame, a MEP examines it to ensure that the frame's maintenance domain level is the same as its own maintenance domain level. The *period* field in the frame indicates the period at which the AIS frames can be expected. When a MEP receives an AIS frame, it detects the defect condition. After detection, when no AIS frames are received within an interval of 3.5 times—the AIS transmission period indicated in the AIS frames received—the MEP clears the AIS defect condition. When the AIS condition is cleared and defects still exist, then the MEPs continue to report alarms.
- AIS PDU format—The fields of the AIS PDU format are:



a. MEG Level—Also called the maintenance domain level, it is a 3-bit field that is used to carry the maintenance domain level of the client MEG.

b. Version—Value is always 0.

c. OpCode—Value for this PDU type is AIS (33).

d. Flags—The first five bits are reserved and are set to 0. The 3-bit information element carried in the three least significant bits are referred to as the period that contains the value of AIS transmission periodicity as illustrated in Table 22 on page 290:

Table 22: AIS Transmission Periodicity

Flags [3:1]	Period Value	Comments
000-011	Invalid value	Invalid value for AIS
100	1s	1 frame per second
101	Invalid value	Invalid value for AIS
110	1 min	1 frame per minute
111	Invalid value	Invalid value for AIS

e. TLV offset—Set to 0.

f. End TLV—All-zeroes octet value.

- Server layer and client layer—These layers are part of the ITU-T Recommendation G.805 transport network functional model. This model is based on the concept of layering within a transport network. A transport network is divided into several independent transport layer networks that have a client-server association between adjacent layer networks.
- Maintenance domain—To enable connectivity fault management (CFM) on an Ethernet interface, maintenance domains, maintenance associations, and maintenance end points (MEPs) are created and configured in a network. You can configure up to eight maintenance domain levels in a network. Each maintenance domain level is a part of the network where the connectivity issues can be monitored and corrected. Provider domain and customer domain are some examples for maintenance domains. Each maintenance domain has a maintenance association. Each maintenance association includes MEPs and maintenance intermediate points (MIPs) in that domain. The MEPs are located at the boundary of the domain and the MIPs are located within the domain. MEPs generate and transmit continuity check messages (CCMs) at configured intervals to the entire maintenance association to check the connectivity in the network.
- Ethernet services (ETH) layer—A layer in the metro Ethernet network model, where this layer is responsible for the OAM services that are required to support the Ethernet services in the network.

SEE ALSO

show oam ethernet connectivity-fault-management interfaces

show oam ethernet connectivity-fault-management mep-statistics | **2764**

Ethernet Alarm Indication Signal Overview

ACX Series routers support ITU-T Y.1731 Ethernet Alarm Indication Signal function (ETH-AIS) to provide fault management for service providers. ETH-AIS enables you to suppress alarms when a fault condition is detected. Using ETH-AIS, an administrator can differentiate between faults at customer level or faults at provider level.

The advantage of ETH-AIS is:

- Customers need not raise alarms due to lower level failures.
- Customers can get refund based on service unavailability.

When a fault condition is detected, a maintenance end point (MEP) generates ETH-AIS packets to the configured client levels for a specified duration until the fault condition is cleared. Any MEP configured to generate ETH-AIS packets signals to a level higher than its own. A MEP receiving ETH-AIS recognizes that the fault is at a lower level and then suppresses alarms at current level.

ACX Series routers support ETH-AIS PDU generation for server MEPs based on the following defect conditions:

- Loss of connectivity (physical link loss detection)
- Layer 2 circuit or Layer 2 VPN down

Alarm indication signaling is done through the transmission and propagation of ETH-AIS PDUs. ETH-AIS should be enabled on MEPs. A MEP which is configured to issue packets with ETH-AIS information is generally of server layer and continues to transmit periodic packets with ETH-AIS information until the defect condition is cleared. CFM MEPs, upon receiving ETH-AIS PDUs, suppresses loss of continuity alarms associated with its peer MEPs. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of an ETH-AIS condition.

For point-to-point Ethernet connectivity, a MEP has only a single peer MEP. Therefore, a MEP suppress alarms on its peer MEP when it receives the ETH-AIS information.

For multi-point Ethernet connectivity, a MEP which receives ETH-AIS information cannot determine the exact MEP encountered a fault condition and therefore it will not be able to isolate the exact peer MEP for alarm suppression. ITU-T Y.1731 recommends suppressing alarms for all peer MEPs irrespective of the connectivity status.

AIS transmission—A MEP upon detecting a defect condition transmits ETH-AIS PDUs in a direction opposite to its peer MEPs. The transmission of ETH-AIS PDUs is based on a configured ETH-AIS transmission period. An ETH-AIS transmission period of 1 second is recommended. The first ETH-AIS PDU must be transmitted immediately following the detection of a defect condition.

AIS reception—A MEP upon receiving ETH-AIS PDUs examines it to ensure that its maintenance domain (MD) level corresponds to the same MD level. Upon receiving an ETH-AIS PDU, the MEP detects a defect condition. Following the detection of a defect condition, if there are no ETH-AIS PDUs received within an interval of 3.5 times the ETH-AIS transmission period indicated in the ETH-AIS PDUs received earlier, the MEP clears the defect condition. After the fault condition is cleared, MEPs continue to report alarms.

NOTE: ACX Series routers do not support ITU-T Y.1731 ETH-AIS for layer 2 services (bridging).

The following are the limitations for server MEP

- Triggering of ETH-AIS messages over services (Layer 2 circuit and Layer 2 VPN) by the link-loss server MEP is done on a best-effort manner. This is because the transmission of ETH-AIS messages is independent of the service status and there is no guarantee for delivering the ETH-AIS messages before service goes down.
- Pseudowire protection with CFM-MEP session is not monitored by the server-MEP because an entity to monitor pseudowire protection already exists for the service (Layer 2 circuit and Layer 2 VPN).

SEE ALSO

show oam ethernet connectivity-fault-management mep-statistics

Configuring ETH-AIS on a CFM MEP

MX Series routers support ITU-T Y.1731 Ethernet alarm indication signal (ETH-AIS) function to provide fault management for service providers. ETH-AIS enables the service provider to suppress alarms when a fault condition is detected.

The following points are to be noted when ETH-AIS is configured in a maintenance domain:

- Transmitting or receiving of AIS on a MEP does not override the **lowest-priority-defect** statement configured at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id*]** hierarchy level. Therefore, alarms are reported according to the defect priority configured.
- Alarms are reported even when the higher domain levels exchange CCMs at a faster rate than the lower domain levels.
- Maintenance association intermediate point (MIP) is transparent to ETH-AIS frames—that is, the MIPs do not perform any action in response to ETH-AIS frames.
- When the service provider requests the MEP to generate an AIS for a lower level or for the same level, the request is rejected.

- AIS generation is stopped when the MEP clears the remote MEP within the maintenance association.
- When the **auto-discovery** statement is enabled for a MEP, the remote MEP information is cleared after the configured hold interval expires.

The following tasks explain how to enable ETH-AIS in a maintenance domain, configure an action to be taken when a defect is detected, and to attach the action profile to a CFM MEP:

1. Configuring an Action Profile | 293
2. Configuring an Action to Be Taken When an AIS Alarm Is Detected | 294
3. Attaching the Action Profile to a CFM MEP | 295

Configuring an Action Profile

To configure an action profile for ETH-AIS:

1. Go to the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
```

2. Configure an action profile to use when one or more remote MEPs are down.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# edit action-profile action-profile-name
```

3. Configure an event that needs to be monitored.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name]
user@host# edit event
```

4. Configure the defect condition that generates an alarm indication signal.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event]
user@host# edit ais-trigger-condition
```

5. Configure the **adjacency-loss** statement to inform the operator when the physical connectivity is lost between the peer MEPs.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
  ais-trigger-condition]
```

```
user@host# set adjacency-loss
```

6. Configure the **all-defects** statement to inform the operator that all possible defects must be considered to raise the alarm indication signal.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
user@host# set all-defects
```

7. Configure the **cross-connect-ccm** statement to inform the operator when cross-connect continuity check messages (CCMs) are received by the MEP and to raise an alarm indication signal in response.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
user@host# set cross-connect-ccm
```

8. Configure the **erroneous-ccm** statement to inform the operator when CCMs with unexpected MEP ID or maintenance domain level are received by the MEP and an AIS alarm is raised in response.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
user@host# set erroneous-ccm
```

9. Configure the **receive-ais** statement to inform the operator that an AIS message has been received from the peer MEP in its own maintenance level.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
user@host# set receive-ais
```

Configuring an Action to Be Taken When an AIS Alarm Is Detected

Configure an action to be taken when an AIS alarm is detected.

1. Go to the **[edit protocols oam ethernet connectivity-fault-management action-profile *action-profile-name* action]** hierarchy level.

```
[edit]
```

```
user@host# edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
  action
```

2. Configure the **log-and-generate-ais** statement to log the event that generated the AIS message.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action]
user@host# edit log-and-generate-ais
```

3. Configure the interval between AIS messages that are to be received by the MEP as 1 minute or 1 second.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action
  log-and-generate-ais]
user@host# set interval (1m | 1s)
```

4. Configure the server maintenance domain level range of the MEP from 1 through 7.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action
  log-and-generate-ais]
user@host# set level level
```

5. Configure the 802.1p priority of the AIS packet from 1 through 7.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action
  log-and-generate-ais]
user@host# set priority level
```

Attaching the Action Profile to a CFM MEP

After configuring an event and an action to be monitored in an action profile, you must attach the action profile to a CFM MEP.

1. Go to the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
```

2. Configure the maintenance domain with a name.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# edit maintenance-domain md-name
```

3. Configure the maintenance domain with a client maintenance entity group (MEG) level or maintenance association level—the level which the client layer maintenance association intermediate point (MIPs) and the MEPs exist—from 0 through 7.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# edit level level
```

> **NOTE:** You cannot configure a maintenance domain level that is lower than or equal to the maintenance association level that it is associated with.

4. Configure the maintenance association.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# edit maintenance-association ma-name
```

5. Configure the continuity check that is performed on all the MEPs in a domain level by sending CCMs with an interval between two CCMs—100 miiliseconds, 10 milliseconds, 1 second, 10 seconds, 1 minute, or 10 minutes—and the number of CCMs that are to be lost before marking a MEP as down.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
  maintenance-association ma-name]
user@host# set continuity-check interval (100ms | 10m | 10ms | 1m | 1s)
user@host# set continuity-check loss-threshold value
```

6. Configure the MEP with an identifier from 1 through 8192.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
  maintenance-association ma-name]
user@host# set mep mep-id
```

7. Attach the configured action profile to the MEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id]
user@host# set action-profile action-profile-name
```

8. Configure the interface of the MEP over which the CCMs are transmitted.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id]
user@host# set interface interface-name
```

9. Configure the direction for the CCMs to travel to the next MEP as up or down.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id]
user@host# set direction (down | up)
```

10. Configure the 802.1p priority for the CCMs and link-trace packet from 0 through 7.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name mep mep-id]
user@host# set priority priority-value
```

SEE ALSO

ITU-T Y.1731 Ethernet Service OAM Overview | 165

Ethernet Alarm Indication Signal Overview | 291

Configuring Alarm Indication Signal on ACX Series Routers

ACX Series routers support ITU-T Y.1731 Ethernet Alarm Indication Signal function (ETH-AIS) to provide fault management for service providers. ETH-AIS enables you to suppress alarms when a fault condition is detected.

To support ETH-AIS transmission, the following configuration information is required by a CFM MEP:

- Client Maintenance Entity Group level—Maintenance Entity Group (MEG) level at which the immediate client layer Maintenance Domain Intermediate Points (MIPs) and Maintenance Association End Points (MEPs) exist.

- ETH-AIS transmission period—Determines the ETH-AIS PDU transmission interval.
- Priority—Determines the priority of packets with ETH-AIS information. This is optional.

To configure ETH-AIS in CFM MEP, you need to:

- Configure an action profile with ETH-AIS action
- Attach the action profile to the CFM MEP

To configure an action profile with ETH-AIS action, include the following statements at the [edit protocols oam ethernet connectivity-fault-management] hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile action-profile-name {
    event {
        adjacency-loss;
        all-defects;
        cross-connect-ccm;
        errored-ccm;
        receive-ais;
    }
    action {
        log-and-generate-ais {
            level [1-7];
            interval 1s | 1m ;
            priority [0-7];
        }
        log-ais;
    }
}
```

To attach an action profile to a CFM MEP, include the following statements at the [edit protocols oam ethernet connectivity-fault-management] hierarchy level:

```
maintenance-domain maintenenace-domain-name {
level level-number;
    maintenance-association maintenance-domain-name {
        continuity-check {
            interval 1s;
            loss-threshold 3;
        }
        mep mep-id {
            interface interface-name;
            direction up | down;
            priority priority-value;
```

```
            action-profile action-profile-name;
        }
    }
}
```

NOTE: You cannot configure a maintenance domain level that is lower than or equal to the level that it is associated with.

To support ETH-AIS transmission, the following configuration information required by a server MEP:

- Server MEP definition—Defines the association of server MEP identifier to the server layer.
  - For Layer 2 circuit and Layer 2 VPN, the logical interface connected to a customer network (UNI) would be the identifier for the server layer that needs to be monitored by the server MEP.
  - For physical link loss detection, the physical interface under Ethernet protocol would be the identifier for the server layer that needs to be monitored by the server MEP.
- Association of server MEP defect—Defines the association of server MEP defects to ETH-AIS action.
- Association action profile and server MEP—Defines the binding of server MEP and action profile.

To configure ETH-AIS in server MEP, you need to:

- Create an action profile with ETH-AIS action for server MEP defects.
- Attach the action profile to a server MEP

To create an action profile, include the following statements at the [edit protocols oam ethernet connectivity-fault-management] hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile action-profile-name {
    event {
        server-mep-defects {
            link-loss-defect;
            l2circuit-defect;
            l2vpn-defect;
        }
    }
    action {
        log-and-generate-ais {
            level 1...n;
            interval 1 second | 1 minute;
```

```
            priority dot1p [range 0-7];
        }
    }
}
```

To attach an action profile to a server MEP, include the following statement at the [edit protocols oam ethernet connectivity-fault-management] hierarchy level:

```
[edit protocols oam ethernet connectivity-fault-management]
server-mep mep-identifier {
    protocol l2circuit | l2vpn | ethernet {
        interface interface-name;
    }
    action-profile action-profile-name;
}
```

SEE ALSO

- ITU-T Y.1731 Ethernet Service OAM Overview | **165**
- Ethernet Alarm Indication Signal Overview | **291**

RELATED DOCUMENTATION

- ITU-T Y.1731 Ethernet Service OAM Overview | **165**
- Configuring Ethernet Frame Delay Measurement Sessions | **185**
- Configuring Ethernet Frame Loss Measurement | **223**
- Configuring Connectivity Fault Management (CFM) | **29**

Inline Transmission Mode

IN THIS SECTION

- Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling | **301**
- Enabling Inline Transmission of Link Fault Management Keepalives for Maximum Scaling | **302**
- Enabling Inline Mode Of Performance Monitoring To Achieve Maximum Scaling | **306**

Supported Inline CCM and Inline PM Scaling Values | 309
Enabling the Hardware-Assisted Timestamping Option | 311

Use this topic to understand what inline transmission is and how to enable it for maximum scaling for CFM, LFM, and performance monitoring functions.

Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling

Scaling is the ability of a system to handle increasing amounts of work and to continue to function well. Scaling can refer to increasing capacity and the ability to handle increasing workload, number of subscribers or sessions, hardware components, and so on. Continuity check protocol is used for fault detection within a maintenance association. The maintenance association end points (MEPs) send continuity check messages (CCMs) periodically. The time between the transmissions of CCMs is known as the interval. The receiving MEP maintains a database of all MEPs in the maintenance association.

By default, CCMs are transmitted by the CPU of a line card, such as a Modular Port Concentrator (MPC). If the duration between transmissions of CCMs is low or if the CCMs for a specific line card scale, then we recommend that you delegate transmission of CCMs to the forwarding ASIC (that is, to the hardware) by enabling inline transmission of CCMs. Inline transmission of CCMs is also known as inline keepalives or Inline-KA. Inline transmission enables the system to handle more connectivity fault management (CFM) sessions per line card. By enabling inline transmission of CCMs, you can achieve maximum scaling of CCMs.

To enable inline transmission of CCMs, perform the following steps:

1. In configuration mode, go to the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Delegate transmission of CCMs to hardware by enabling hardware-assisted keepalives.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

> **NOTE:** Inline transmission of CCMs is not enabled when there is a CFM session already established. To enable inline transmission, you must first deactivate the CFM session using the **deactivate** command and then reactivate the CFM session using the **activate** command.

To disable inline transmission, use the **hardware-assisted-keepalives** **disable** statement. After disabling inline transmission, you must reboot the router for the changes to take effect.

SEE ALSO

Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades | 75

Enabling Inline Transmission of Link Fault Management Keepalives for Maximum Scaling

Scaling is the ability of a system to handle increasing amounts of work and to continue to function well. Scaling can refer to increasing capacity and the ability to handle increasing workload, number of subscribers or sessions, hardware components, and so on.

By default, LFM keepalive packets are transmitted by the periodic packet management **ppm** process on the line-card. You can delegate transmission of LFM keepalive packets to the forwarding ASIC (that is, to the hardware) by enabling inline transmission. Inline transmission of LFM keepalives is also known as inline keepalives or Inline-KA. By enabling inline transmission of LFM keepalive packets, you can achieve maximum scaling of keepalive packets, reduction of the load on the **ppm** process, and support LFM in-service software upgrade (ISSU) for non-juniper peers (for a keepalive interval of 1 second).

> **NOTE:** Do not enable or disable inline transmission of LFM when an LFM session is already established. To enable or disable inline transmission, you must first deactivate the existing established LFM session using the **deactivate** command, and then reactivate the LFM session using the **activate** command after enabling or disabling inline LFM.

Before you enable inline transmission of LFM keepalive packets, complete the following tasks:

- Verify if any LFM session is online and active. To verify if any existing or established LFM session is online and active, issue the following command:

  ```
  user@host> show oam ethernet link-fault-management detail
  ```

```
Oct 18 02:04:17
  Interface: ge-0/0/0
    Status: Running, Discovery state: Active Send Local
    Transmit interval: 1000ms, PDU threshold: 3 frames, Hold time: 0ms
    Peer address: 00:00:00:00:00:00
    Flags:0x8
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 28, Event: 0, Variable request: 0, Variable response: 0  =
after waiting for a while count increased by 15
      Loopback control: 0, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Disabled, Loop status: Unknown
    Detect LOC: Disabled, LOC status: Unknown
```

The OAM transmit statistics reflect that the **ppm** process is handling the transmission of LFM keepalive packets.

- Deactivate the LFM session so that you can enable inline LFM mode. To deactivate the LFM session, issue the following command:

```
[edit]
user@host # deactivate protocols oam ethernet link-fault-management interface interface-name
```

- Commit the configuration. To commit the configuration, issue the following command:

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

To enable inline transmission of LFM keepalive packets, perform the following steps:

1. In configuration mode, go to the **[edit protocols oam ethernet link-fault-management]** hierarchy level.

```
[edit]
user@host# edit protocols oam ethernet link-fault-management
```

2. Delegate transmission of LFM keepalive packets to hardware by enabling hardware-assisted keepalives.

```
[edit protocols oam ethernet link-fault-management]
user@host# set hardware-assisted-keepalives
```

3. Commit the configuration.

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

4. Re-activate the LFM session as follows:

```
[edit]
user@host # activate protocols oam ethernet link-fault-management interface interface-name
```

5. Commit the configuration.

```
[edit]
```

```
user@host # commit
```

6. Verify that the trasnmission of LFM keepalive packets is delegated from the **ppm** process to the hardware. To verify that you have enabled inline transmission, issue the following command:

   `user@host>` **show oam ethernet link-fault-management detail**

```
Oct 18 02:05:05
  Interface: ge-0/0/0
    Status: Running, Discovery state: Active Send Local
    Transmit interval: 1000ms, PDU threshold: 3 frames, Hold time: 0ms
    Peer address: 00:00:00:00:00:00
    Flags:0x8
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 1, Event: 0, Variable request: 0, Variable response: 0  =
even after 10 seconds count is still 1
      Loopback control: 0, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
```

```
    Events: 0, Window: 0, Threshold: 1
    Errors in period: 0, Total errors: 0
  Loopback tracking: Disabled, Loop status: Unknown
  Detect LOC: Disabled, LOC status: Unknown
```

The OAM transmit statistics are not updated. When you enable inline transmission of LFM keepalive packets, the OAM transmit statistics are not updated.

To disable inline LFM, verify if any existing established LFM session is online and active. Deactivate the LFM session and commit. Disable inline LFM by deleting the **hardware-assisted-keepalives** statement and commit. Then, reactivate LFM session and commit the configuration.

SEE ALSO

hardware-assisted-keepalives (lfm)

Enabling Inline Mode Of Performance Monitoring To Achieve Maximum Scaling

Performance monitoring is useful for studying the traffic pattern in a network over a period of time. It helps to identify network problems before you are impacted by network defects.

By default, performance monitoring packets are handled by the CPU of a line-card, such as Modular Port Concentrator (MPC). Enabling inline mode of performance monitoring delegates the processing of the protocol data units (PDUs) to the forwarding ASIC (that is, to the hardware). By enabling inline mode of performance monitoring, the load on the CPU of the line-card is reduced and you can configure an increased number of performance monitoring sessions and achieve maximum scaling for service OAM performance monitoring sessions. On MX Series routers, you can configure inline mode of performance monitoring only if the network services mode on the router is configured to **enhanced-ip** and enhanced connectivity fault management (**enhanced-cfm-mode)**) is configured.

By enabling inline mode of performance monitoring, you can achieve maximum scaling for performance monitoring sessions. To achieve maximum scaling for performance monitoring sessions, you must enable scaling of continuity check messages (CCMs) sessions. To enable scaling of CCM sessions, enable inline transmission of continuity check messages. For more information on inline transmission of continuity check messages, see “Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling” on page 301. To view the supported scaling values for CCM and PM, see “Supported Inline CCM and Inline PM Scaling Values” on page 309.

Inline mode of performance monitoring is supported only for proactive mode of frame delay measurement (Two-way Delay Measurements) and synthetic loss measurements (SLM)sessions. Performance monitoring functions configured using the iterator profile (CFM)are referred to as proactive performance monitoring.

Inline mode of performance monitoring for frame loss measurement using service frames (LM) is not supported.

> **NOTE:** MPC3E (MX-MPC3E-3D) and MPC4E (MPC4E-3D-32XGE-SFPP and MPC4E-3D-2CGE-8XGE) do not support inline mode of performance monitoring. User-defined Data TLV is not supported if you have configured inline mode of performance monitoring. Also, only 12 history records per PM sessions are supported.
>
> We recommend that you enable inline mode of performance monitoring before you configure the performance monitoring sessions as the change may interfere with the existing performance monitoring sessions.

To enable inline mode of performance monitoring, perform the following steps:

1. In configuration mode, go to the **[edit chassis]** hierarchy level and configure the network services mode of the router. The network service mode of the router must be configured as **enhanced ip** to enable enhanced connectivity fault management (CFM) mode.

   > **NOTE:** If the network services mode is not **enhanced-ip**, and you have enabled enhanced CFM, the following warning message is displayed:
   > **[edit protocols oam ethernet]**
   > **'connectivity-fault-management'**
   > **enhanced ip is not effective please configure enhanced ip and give router reboot**

   ```
   [edit chassis]
   user@host# set network-services enhanced-ip
   ```

2. In configuration mode, go to the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level and enable enhanced connectivity fault management mode by using the **enhanced-cfm-mode** option.

   ```
   [edit]
   user@host# set protocols oam ethernet connectivity-fault-management enhanced-cfm-mode
   ```

3. In configuration mode, go to the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level. Configure the enhanced iterator profile by using the **enhanced-sla-iterator** option and specify the measurement interval by using the **measurement-interval** option.

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
    enhanced-sla-iterator measurement-interval value
```

4. Enable inline performance monitoring.

> **NOTE:** You can enable inline mode of performance monitoring for both the originator and the responder of the service OAM performance monitoring sessions by using the **hardware-assisted-pm** command.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-pm
```

5. (Optional) Enable inline transmission of CCMs to enable better scaling if inline transmission of CCMs is not automatically enabled.

> **NOTE:** You can achieve better scaling if both inline performance monitoring and inline transmission of CCMs is enabled.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

6. Commit the configuration.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# commit
```

SEE ALSO

Enabling Enhanced Connectivity Fault Management Mode | 71

Network Services Mode Overview

hardware-assisted-pm

Supported Inline CCM and Inline PM Scaling Values

This topic lists the scaling values for inline mode of performance monitoring and inline transmission of continuity check messages. The scaling values are based on the different cycle-time interval values. Each table lists the maximum number of connectivity fault management (CFM) sessions and performance monitoring (PM) sessions per line card and per chassis when you configure inline CCM, enhanced CFM, and enhanced PM by using the **hardware-assisted-keepalives**, **enhanced-cfm-mode**, and **hardware-assisted-pm** options.

> **NOTE:** The scaling values do not consider the load from other protocols in the system and so the actual realized scaling values for line card and chassis vary depending on other protocol configurations and scaling in the system. We recommend that you configure DDoS for CFM. Limit the number of CFM packets, that are sent to the CPU of the line card, to 3000. Limiting the number of packets safeguards the CPU from scaled CFM configurations of various CFM protocol events.

Table 23 on page 309 lists the maximum number of connectivity fault management (CFM) sessions and performance monitoring (PM) sessions per line card and per chassis when you configure both the CCM interval and the PM interval as 1 second.

Table 23: Scaling Values for CFM and PM (CCM Interval: 1 sec and PM Interval: 1 sec)

CFM Line Card Scale	PM Line Card Scale	CFM Chassis Scale	PM Chassis Scale
4000	4500	16000	16000
6000	3750	16000	16000
7000	3375	16000	16000
8000	3000	16000	16000

Table 24 on page 309 lists the maximum number of connectivity fault management (CFM) sessions and performance monitoring (PM) sessions per line card and per chassis when you configure the CCM interval as 1 second and the PM interval as 100 milliseconds.

Table 24: Scaling Values for CFM and PM (CCM Interval: 1 sec and PM interval: 100 ms)

CFM Line Card Scale	PM Line Card Scale	CFM Chassis Scale	PM Chassis Scale
4000	450	12000	4000
6000	375	12000	4000

Table 24: Scaling Values for CFM and PM (CCM Interval: 1 sec and PM interval: 100 ms) *(continued)*

CFM Line Card Scale	PM Line Card Scale	CFM Chassis Scale	PM Chassis Scale
7000	337	12000	4000
8000	300	12000	4000

Table 25 on page 310 lists the maximum number of connectivity fault management (CFM) sessions and performance monitoring (PM) sessions per line card and per chassis when you configure the CCM interval as 100 milliseconds and the PM interval as 1 second.

Table 25: Scaling Values for CFM and PM (CCM Interval: 100 ms and PM interval: 1 sec)

CFM Line Card Scale	PM Line Card Scale	CFM Chassis Scale	PM Chassis Scale
4000	3000	8000	6000
3000	3750	8000	6000
2000	4500	8000	6000
1000	4500	8000	6000

Table 26 on page 310 lists the maximum number of connectivity fault management (CFM) sessions and performance monitoring (PM) sessions per line card and per chassis when you configure both the CCM interval and the PM interval as 100 milliseconds.

Table 26: Scaling Values for CFM and PM (CCM Interval: 100 ms and PM interval: 100 ms)

CFM Line Card Scale	PM Line Card Scale	CFM Chassis Scale	PM Chassis Scale
4000	300	8000	3000
3000	375	8000	3000
2000	450	8000	3000
1000	450	8000	3000

SEE ALSO

enhanced-cfm-mode | **1789**

hardware-assisted-pm

Enabling the Hardware-Assisted Timestamping Option

By default, Ethernet frame delay measurement uses software for timestamping transmitted and received ETH-DM frames. For Ethernet interfaces, you can optionally use hardware timing to assist in the timestamping of received ETH-DM frames to increase the accuracy of delay measurements.

Enabling hardware-assisted timestamping of received frames can increase the accuracy of ETH-DM calculations when the DPC is loaded with heavy traffic in the receive direction.

To enable Ethernet frame delay measurement hardware assistance on the reception path, include the **hardware-assisted-timestamping** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            performance-monitoring {
                hardware-assisted-timestamping;
            }
        }
    }
}
```

SEE ALSO

hardware-assisted-timestamping | 1796

RELATED DOCUMENTATION

Introduction to OAM Connectivity Fault Management (CFM) | 22

Configuring Continuity Check Messages | 124

Introduction to OAM Link Fault Management (LFM) | 131

CHAPTER 6

Ethernet OAM Connectivity Fault Management for Switches

IN THIS CHAPTER

- Understanding Ethernet OAM Connectivity Fault Management for Switches | 312
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches | 315
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Understanding Ethernet OAM Connectivity Fault Management for Switches

Ethernet interfaces on Juniper Networks Switches and Juniper Networks Junos operating system (Junos OS) for switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM). CFM monitors Ethernet networks that might comprise one or more service instances for network-compromising connectivity faults.

The major features of CFM are:

- Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN level.
- Path discovery and fault verification using the linktrace protocol.
- Fault isolation using the loopback protocol.

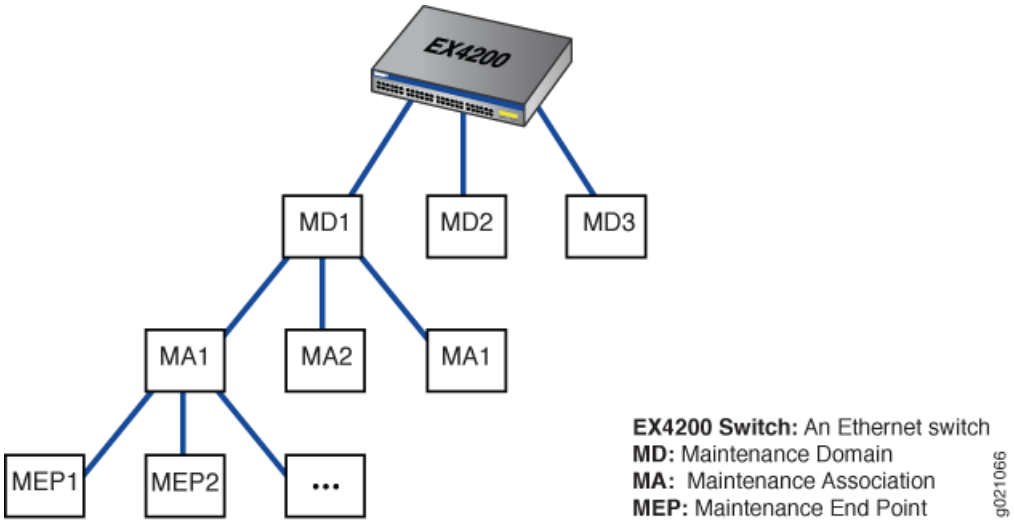
CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains. Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible.

In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought of as a full mesh of maintenance association endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages. There is also a maintenance intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outer domains are assigned a higher level than the inner domains. Configure customer end points to have the highest maintenance domain level. The maintenance domain level is a mandatory parameter that indicates the nesting relationships between various maintenance domains. The level is embedded in each CFM frame. CFM messages within a given level are processed by MEPs at that same level.

To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and maintenance association end points (MEPs). Figure 20 on page 313 shows the relationships among maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs) configured on a switch.

Figure 20: Relationship Among MEPs, MIPs, and Maintenance Domain Levels



CFM Limitations on EX4600 Switches

Starting in Junos OS Release 18.3R1, Junos OS provides CFM support on EX4600. CFM support on EX4600 has the following limitations:

- CFM support is provided via software using filters. This can impact scaling.
- Inline Packet Forwarding Engine (PFE) mode is not supported. In Inline PFE mode, you can delegate periodic packet management (PPM) processing to the Packet Forwarding Engine (PFE) which results in faster packet handling and the CCM interval supported is 10 milliseconds.
- Performance monitoring (ITU-T Y.1731 Ethernet Service OAM) is not supported.
- CCM interval of less than 1 second is not supported.
- CFM is not supported on Routed Interfaces and aggregated Ethernet (lag) interfaces.

- MIP half function, to divide the MIP functionality into two unidirectional segments to improve network coverage, is not supported.
- Up MEP is not supported.
- Total number of CFM sessions supported is 20.

CFM Limitations on QFX5200 Switches and QFX5210 Switches

Starting in Junos OS Release 18.4R1, Junos OS provides CFM support on QFX5200 switches and QFX5210 switches. CFM support on QFX5200 switches and QFX5210 switches has the following limitations:

- CFM support is provided via software using filters. This can impact scaling.
- Inline Packet Forwarding Engine (PFE) mode is not supported. In Inline PFE mode, you can delegate periodic packet management (PPM) processing to the Packet Forwarding Engine (PFE) which results in faster packet handling and the CCM interval supported is 10 milliseconds.
- Performance monitoring (ITU-T Y.1731 Ethernet Service OAM) is not supported.
- CCM interval of less than 1 second is not supported.
- CFM is not supported on Routed Interfaces and aggregated Ethernet (lag) interfaces.
- MIP half function, to divide the MIP functionality into two unidirectional segments to improve network coverage, is not supported.
- Up MEP is not supported.
- Total number of CFM sessions supported is 20.

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | **320**

Junos OS Network Interfaces Configuration Guide

Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches

IN THIS SECTION

- Requirements | 315
- Overview and Topology | 315
- Configuring Ethernet OAM Connectivity Fault Management on Switch 1 | 315
- Configuring Ethernet OAM Connectivity Fault Management on Switch 2 | 317
- Verification | 319

Ethernet interfaces on EX Series switches and Junos OS for EX Series switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM).

This example describes how to enable and configure OAM CFM on a Gigabit Ethernet interface:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 10.2 or later for EX Series switches
- Two EX Series switches connected by a point-to-point Gigabit Ethernet link

Overview and Topology

CFM can be used to monitor the physical link between two switches. In the following example, two switches are connected by a point-to-point Gigabit Ethernet link. The link between these two switches is monitored using CFM.

Configuring Ethernet OAM Connectivity Fault Management on Switch 1

CLI Quick Configuration

To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
```

set name-format character-string

set maintenance-domain private level 0

set maintenance-association private-ma

set continuity-check hold-interval 1s

Step-by-Step Procedure

To enable and configure OAM CFM on switch 1:

1. Specify the maintenance domain name format:

   ```
   [edit protocols oam ethernet connectivity-fault-management
   maintenance-domain]
   user@switch1# set name-format character-string
   ```

2. Specify the maintenance domain name and the maintenance domain level:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch1# set maintenance-domain private level 0
   ```

3. Create a maintenance association:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   private]
   user@switch1# set maintenance-association private-ma
   ```

4. Enable the continuity check protocol and specify the continuity check hold interval:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   private maintenance-association private-ma]
   user@switch1# set continuity-check hold-interval 1s
   ```

5. Configure the maintenance association end point (MEP):

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   private maintenance-association private-ma]
   user@switch1# set mep 100 interface ge-1/0/1 auto-discovery direction down
   ```

Results

Check the results of the configuration.

```
[edit]

user@switch1 > show
```

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 100 {
                            interface ge-1/0/1;
                            auto-discovery;
                            direction down;
                        }
                    }
                }
            }
        }
    }
```

Configuring Ethernet OAM Connectivity Fault Management on Switch 2

CLI Quick Configuration

To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
set name-format character-string
set maintenance-domain private level 0
set maintenance-association private-ma
set continuity-check hold-interval 1s
```

Step-by-Step Procedure

The configuration on switch 2 mirrors that on switch 2.

1. Specify the maintenance domain name format:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch2# set name-format character-string
   ```

2. Specify the maintenance domain name and the maintenance domain level:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   ```

```
user@switch2# set maintenance-domain private level 0
```

3. Create a maintenance association:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
private]
user@switch2# set maintenance-association private-ma
```

4. Enable the continuity check protocol and specify the continuity check hold interval:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
private maintenance-association private-ma]
user@switch2# set continuity-check hold-interval 1s
```

5. Configure the maintenance association end point (MEP)

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
private maintenance-association private-ma]
user@switch2# set mep 200 interface ge-0/2/5 auto-discovery direction down
```

Results

Check the results of the configuration.

```
[edit]
user@switch2 > show
```

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 200 {
                            interface ge-0/2/5;
                            auto-discovery;
                            direction down;
                        }
```

```
        }
      }
    }
  }
```

Verification

IN THIS SECTION

- Verifying That OAM CFM Has Been Configured Properly | **319**

To confirm that the configuration is working properly, perform these tasks:

Verifying That OAM CFM Has Been Configured Properly

Purpose

Verify that OAM CFM has been configured properly.

Action

Use the **show oam ethernet connectivity-fault-management interfaces detail** command:

```
user@switch1# show oam ethernet connectivity-fault-management interfaces detail
```

Sample Output

```
Interface name: ge-1/0/1.0, Interface status: Active, Link status: Up
  Maintenance domain name: private, Format: string, Level: 0
    Maintenance association name: private-ma, Format: string
    Continuity-check status: enabled, Interval: 1ms, Loss-threshold: 3 frames
    MEP identifier: 100, Direction: down, MAC address: 00:90:69:0b:4b:94
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : yes
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : yes
    Statistics:
```

```
    CCMs sent                                    : 76
    CCMs received out of sequence                : 0
    LBMs sent                                    : 0
    Valid in-order LBRs received                 : 0
    Valid out-of-order LBRs received             : 0
    LBRs received with corrupted data            : 0
    LBRs sent                                    : 0
    LTMs sent                                    : 0
    LTMs received                                : 0
    LTRs sent                                    : 0
    LTRs received                                : 0
    Sequence number of next LTM request          : 0
  Remote MEP count: 2
    Identifier    MAC address        State    Interface
     2001     00:90:69:0b:7f:71       ok    ge-0/2/5.0
```

Meaning

When the output displays that continuity-check status is **enabled** and displays details of the remote MEP, it means that connectivity fault management (CFM) has been configured properly.

RELATED DOCUMENTATION

Understanding Ethernet OAM Connectivity Fault Management for Switches | **312**

Junos OS Network Interfaces Configuration Guide

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure)

Ethernet interfaces on Juniper Networks EX Series Ethernet Switches and Juniper Networks Junos OS for EX Series switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM).

NOTE: This feature is not supported on EX4300 switches on aggregated Ethernet (LAG) interfaces.

This topic describes these tasks:

1. Creating the Maintenance Domain | **321**
2. Configuring the Maintenance Domain MIP Half Function | **322**
3. Creating a Maintenance Association | **322**
4. Configuring the Continuity Check Protocol | **322**
5. Configuring a Maintenance Association End Point | **323**
6. Configuring a Connectivity Fault Management Action Profile | **325**
7. Configuring the Linktrace Protocol | **325**

Creating the Maintenance Domain

A maintenance domain comprises network entities such as operators, providers, and customers. To enable connectivity fault management (CFM) on an Ethernet interface, you must create a maintenance domains, maintenance associations, and MEPs.

To create a maintenance domain:

1. Specify a name for the maintenance domain:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch# set maintenance-domain domain-name
   ```

2. Specify a format for the maintenance domain name. If you specify **none**, no name is configured:

   - A plain ASCII character string
   - A domain name service (DNS) format
   - A media access control (MAC) address plus a two-octet identifier in the range 0 through 65,535
   - **none**

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   domain-name]
   user@switch# set name-format format
   ```

   For example, to specify the name format as MAC address plus a two-octet identifier:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   domain-name]
   user@switch# set name-format mac+2oct
   ```

3. Configure the maintenance domain level, which is used to indicate the nesting relationship between this domain and other domains. Use a value from 0 through 7:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]
user@switch# set level level
```

Configuring the Maintenance Domain MIP Half Function

> **NOTE:** MIP Half Function (MHF) is not supported on EX4600, QFX5200, and QFX5210 switches.

MIP Half Function (MHF) divides the maintenance association intermediate point (MIP) functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loop-back and link-trace messages to help isolate faults. Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be the same.

To configure the MIP half function:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]
user@switch# set mip-half-function (none | default | explicit)
```

Creating a Maintenance Association

In a CFM maintenance domain, each service instance is called a maintenance association.

To create a maintenance association:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]
user@switch# set maintenance-association ma-name
```

Configuring the Continuity Check Protocol

The continuity check protocol is used for fault detection by a maintenance association end point (MEP) within a maintenance association. The MEP periodically sends continuity check multicast messages. The receiving MEPs use the continuity check messages (CCMs) to build a MEP database of all MEPs in the maintenance association.

To configure the continuity check protocol:

1. Enable the continuity check protocol:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]
   user@switch# set continuity-check
   ```

2. Specify the continuity check hold interval. The hold interval is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set hold-interval number
   ```

3. Specify the CCM interval. The interval is the time between the transmission of CCMs. You can specify 10 minutes (10m), 1 minute (1m), 10 seconds (10s), 1 second (1s), 100 milliseconds (100ms), or 10 milliseconds (10ms).

   > **NOTE:** On EX4600, QFX5200, and QFX5210 switches, CCM interval of less than 1 second is not supported.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set interval number
   ```

4. Specify the number of CCMs (that is, protocol data units) that can be lost before the MEP is marked as down. The default number of protocol data units (PDUs) is 3.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set loss-threshold number
   ```

Configuring a Maintenance Association End Point

To configure a maintenance association end point:

1. Specify an ID for the MEP. The value can be from 1 through 8191.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]
   user@switch# set mep mep-id]
   ```

2. Enable maintenance endpoint automatic discovery if you want to have the MEP accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id
   user@switch# set auto-discovery
   ```

3. You can specify that CFM packets (CCMs) be transmitted only in one direction for the MEP, that is, the direction be set as **down** so that CCMs are transmitted only out of (not into) the interface configured on this MEP.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
   user@switch# set direction down
   ```

4. Specify the logical interface to which the MEP is attached. It can be either an access interface or a trunk interface. If you specify a trunk interface, the VLAN associated with that interface must have a VLAN ID.

   > **NOTE:** You cannot associate an access interface that belongs to multiple VLANs with the MEP.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
   user@switch# set interface interface-name
   ```

5. You can configure a remote MEP from which CCMs are expected. If autodiscovery is not enabled, the remote MEP must be configured under the **mep** statement. If the remote MEP is not configured under the **mep** statement, the CCMs from the remote MEP are treated as errors.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
   user@switch# set remote-mep mep-id
   ```

Configuring a Connectivity Fault Management Action Profile

You can configure an action profile and specify the action to be taken when any of the configured events occur. Alternatively, you can configure an action profile and specify default actions when connectivity to a remote MEP fails.

To configure an action profile:

1. Specify a name for an action profile:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch# set action-profile profile-name
   ```

2. Configure the action of the action profile:

   ```
   [edit protocols oam ethernet connectivity-fault-management action-profile
   profile-name]
   user@switch# set action interface-down
   ```

3. Configure one or more events under the action profile, the occurrence of which will trigger the corresponding action to be taken:

   ```
   [edit protocols oam ethernet connectivity-fault-management action-profile
   profile-name]
   user@switch# set event event
   ```

   See *Junos OS Network Interfaces Configuration Guide*

Configuring the Linktrace Protocol

The linktrace protocol is used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the **traceroute** command to verify the path between a pair of MEPs under the same maintenance association. Linktrace messages can also be used to verify the path between a MEP and a MIP under the same maintenance domain.

To configure the linktrace protocol:

1. Configure the linktrace path age timer. If no response to a linktrace request is received, the request and response entries are deleted after the age timer expires:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch# set linktrace age time
   ```

2. Configure the number of linktrace reply entries to be stored per linktrace request:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   ```

```
user@switch# set linktrace path-database-size path-database-size
```

RELATED DOCUMENTATION

- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches | **315**
- Understanding Ethernet OAM Connectivity Fault Management for Switches | **312**
- *Junos OS Network Interfaces Configuration Guide*

CHAPTER 7

Ethernet OAM Link Fault Management for Switches

IN THIS CHAPTER

- OAM Link Fault Management | 327

OAM Link Fault Management

IN THIS SECTION

- Understanding Ethernet OAM Link Fault Management | 327
- Configuring Ethernet OAM Link Fault Management | 329
- Example: Configuring Ethernet OAM Link Fault Management | 331

Junos OS allows the Ethernet Interfaces to support the IEEE 802.3ah standard Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The topics discuss the use of Ethernet OAM link fault management, and its configuration details.

For features on EX Series Switches that require license, see Understanding Software Licenses for EX Series Switches. To understand more about Junos OS Software Licensing, see the Juniper Licensing Guide. Please refer to the product Data Sheets accessible from Products & Services for details, or contact your Juniper Account Team or Juniper Partner.

Understanding Ethernet OAM Link Fault Management

Juniper Networks Junos operating system (Junos OS) for Juniper Networks allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even

as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward-compatible with existing Ethernet technology.

Ethernet OAM provides the tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual LAN identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports or a virtual service such as pseudowire.
- Isolate faults over a flat (or single operator) network architecture or nested or hierarchical (or multiprovider) networks.

The following OAM LFM features are supported:

- Discovery and Link Monitoring

  The discovery process is triggered automatically when OAM is enabled on the interface. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard. You can specify the discovery mode used for IEEE 802.3ah OAM support. 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. After the discovery process has been initiated, both sides participate in discovery. The switch performs link monitoring by sending periodic OAM protocol data units (PDUs) to advertise OAM mode, configuration, and capabilities.

  You can specify the number of OAM PDUs that an interface can miss before the link between peers is considered down.

- Remote Fault Detection

  Remote fault detection uses flags and events. Flags are used to convey the following: Link Fault means a loss of signal, Dying Gasp means an unrecoverable condition such as a power failure, and Critical Event means an unspecified vendor-specific critical event. You can specify the periodic OAM PDU sending interval for fault detection. The switch uses the Event Notification OAM PDU to notify the remote OAM device when a problem is detected. You can specify the action to be taken by the system when the configured link-fault event occurs.

- Remote Loopback Mode

  Remote loopback mode ensures link quality between the switch and a remote peer during installation or troubleshooting. In this mode, when the interface receives a frame that is not an OAM PDU or a pause frame, it sends it back on the same interface on which it was received. The link appears to be in the active state. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.

  Junos OS can place a remote DTE into loopback mode (if remote loopback mode is supported by the remote DTE). When you place a remote DTE into loopback mode, the interface receives the remote loopback request and puts the interface into remote loopback mode. When the interface is in remote loopback mode, all frames except OAM PDUs are looped back without any changes made to the frames. OAM PDUs continue to be sent and processed.

Configuring Ethernet OAM Link Fault Management

Ethernet OAM link fault management (LFM) can be used for physical link-level fault detection and management. The IEEE 802.3ah LFM works across point-to-point Ethernet links either directly or through repeaters.

To configure Ethernet OAM LFM using the CLI:

1. Enable IEEE 802.3ah OAM support on an interface:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set interface interface-name
   ```

   > **NOTE:** You can configure Ethernet OAM LFM on aggregated interfaces.

   > **NOTE:** The remaining steps are optional. You can choose which of these features to configure for Ethernet OAM LFM on your switch.

2. Specify whether the interface or the peer initiates the discovery process by configuring the link discovery mode to **active** or **passive** (**active** = interface initiates; **passive** = peer initiates):

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set interface interface-namelink-discovery active
   ```

3. Configure a periodic OAM PDU-sending interval (in milliseconds) for fault detection:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set interface pdu-intervalinterval
   ```

4. Specify the number of OAM PDUs that an interface can miss before the link between peers is considered down:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set interface interface-name pdu-threshold threshold-value
   ```

5. Configure event threshold values on an interface for the local errors that trigger the sending of link event TLVs:

   - Set the threshold value (in seconds) for sending frame-error events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-error count
```

- Set the threshold value (in seconds) for sending frame-period events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-period count
```

- Set the threshold value (in seconds) for sending frame-period-summary events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-period-summary count
```

- Set the threshold value (in seconds) for sending symbol-period events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds symbol-period count
```

> **NOTE:** You can disable the sending of link event TLVs.

To disable the sending of link event TLVs:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name negotiation-options no-allow-link-events
```

6. Create an action profile to define event fault flags and thresholds to be taken when the link fault event occurs. Then apply the action profile to one or more interfaces. (You can also apply multiple action profiles to a single interface.)

   a. Name the action profile:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set action-profile profile-name
   ```

   b. Specify actions to be taken by the system when the link fault event occurs:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch# set action-profile profile-name action syslog

   user@switch# set action-profile profile-name action link-down
   ```

c. Specify events for the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set action-profile profile-name event link-adjacency-loss
```

> **NOTE:** For each action profile, you must specify at least one link event and one action. The actions are taken only when all of the events in the action profile are true. If more than one action is specified, all actions are executed. You can set a low threshold for a specific action such as logging the error and set a high threshold for another action such as system logging.

7. Set a remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes made to the frames. Set the remote DTE in loopback mode (the remote DTE must support remote-loopback mode) and then enable remote loopback support for the local interface.

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name remote-loopback

user@switch# set interface interface-name negotiation-options allow-remote-loopback
```

Example: Configuring Ethernet OAM Link Fault Management

IN THIS SECTION

- Requirements | 332
- Overview and Topology | 332
- Configuring Ethernet OAM Link Fault Management on Switch 1 | 332
- Configuring Ethernet OAM Link Fault Management on Switch 2 | 333
- Verification | 334

Junos OS allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example describes how to enable and configure OAM LFM on a Gigabit Ethernet interface:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.4 or later for EX Series switches
- Two EX3200 or EX4200 switches connected directly

Overview and Topology

Junos OS switches allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example uses two EX4200 switches connected directly. Before you begin configuring Ethernet OAM LFM on two switches, connect the two switches directly through a trunk interface.

Configuring Ethernet OAM Link Fault Management on Switch 1

CLI Quick Configuration

To quickly configure Ethernet OAM LFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management]
set interface ge-0/0/0
set interface ge-0/0/0 link-discovery active
set interface ge-0/0/0 pdu-interval 800
set interface ge-0/0/0 remote-loopback
```

Step-by-Step Procedure

To configure Ethernet OAM LFM on switch 1:

1. Enable IEEE 802.3ah OAM support on an interface:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch1# set interface ge-0/0/0
   ```

2. Specify that the interface initiates the discovery process by configuring the link discovery mode to **active**:

   ```
   [edit protocols oam ethernet link-fault-management]
   user@switch1# set interface ge-0/0/0 link-discovery active
   ```

3. Set the periodic OAM PDU-sending interval (in milliseconds) to 800 on switch 1:

   ```
   [edit protocols oam ethernet link-fault-management]
   ```

```
user@switch1# set interface pdu-interval 800
```

4. Set a remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes made to the frames. Ensure that the remote DTE supports remote loopback mode. To set the remote DTE in loopback mode

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0.0 remote-loopback
```

Results

Check the results of the configuration:

```
[edit]
user@switch1# show
```

```
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/0 {
                    pdu-interval 800;
                    link-discovery active;
                    remote-loopback;
                }
            }
        }
    }
```

Configuring Ethernet OAM Link Fault Management on Switch 2

CLI Quick Configuration

To quickly configure Ethernet OAM LFM on switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management ]
set interface ge-0/0/1
set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Step-by-Step Procedure

To configure Ethernet OAM LFM on switch 2:

1. Enable OAM on the peer interface on switch 2:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1
```

2. Enable remote loopback support for the local interface:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Results

Check the results of the configuration:

```
[edit]
user@switch2# show
```

```
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/1 {
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
```

Verification

Verifying That OAM LFM Has Been Configured Properly

Purpose

Verify that OAM LFM has been configured properly.

Action

Use the **show oam ethernet link-fault-management** command:

```
user@switch1#show oam ethernet link-fault-management
```

Sample Output

```
Interface: ge-0/0/0.0
Status: Running, Discovery state: Send Any
Peer address: 00:19:e2:50:3b:e1
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote entity information:
Remote MUX action: forwarding, Remote parser action: forwarding
Discovery mode: active, Unidirectional mode: unsupported
Remote loopback mode: supported, Link events: supported
Variable requests: unsupported
```

Meaning

When the output displays the MAC address and the discover state is **Send Any**, it means that OAM LFM has been configured properly.

CHAPTER 8

Ethernet Frame Delay

IN THIS CHAPTER

- Understanding Ethernet Frame Delay Measurements on Switches | 336
- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343

Understanding Ethernet Frame Delay Measurements on Switches

IN THIS SECTION

- Ethernet Frame Delay Measurements | 337
- Types of Ethernet Frame Delay Measurements | 337
- Limitations | 338

Performance management depends on the accurate measurement of service-level agreement (SLA) objective parameters, which can include bandwidth and reliability. In many cases, a service provider could be subject to penalties imposed by regulation, statute, or contract if network performance is not within the bounds established for the service. One key performance objective is delay, along with its close relative, delay variation (often called jitter). Some applications (such as bulk file transfer) will function just as well with high delays across the network and high delay variations, while other applications (such as voice) can function only with low and stable delays. Many networks invoke protocols or features available at Layer 3 (the packet layer) or higher to measure network delays and jitter link by link. However, when the network consists of many Ethernet links, there are few protocols and features available at Layer 2 (the frame layer)

that allow routers and switches to measure frame delay and jitter. This is where the ability to configure and monitor Ethernet frame delay is helpful.

This topic includes:

Ethernet Frame Delay Measurements

You can perform Ethernet frame delay measurements (referred to as ETH-DM in Ethernet specifications) on Juniper Networks EX Series Ethernet Switches. This feature allows you to configure on-demand Operation, Administration, and Maintenance (OAM) statements for the measurement of frame delay and frame delay variation (jitter). You can configure Ethernet frame delay measurement in either one-way or two-way (round-trip) mode to gather frame delay statistics simultaneously from multiple sessions. Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor SLAs.

Ethernet frame delay measurement also collects other useful information, such as worst and best case delays, average delay, and average delay variation. It supports software-assisted timestamping in the receive direction for delay measurements. It also provides runtime display of delay statistics when two-way delay measurement is triggered. Ethernet frame delay measurement records the last 100 samples collected per remote maintenance association end point (MEP) or per connectivity fault management (CFM) session. You can retrieve the history at any time using simple commands. You can clear all Ethernet frame delay measurement statistics and PDU counters. Ethernet frame delay measurement is fully compliant with the ITU-T Y.1731 (*OAM Functions and Mechanisms for Ethernet-based Networks*) specification.

Ethernet frame delay measurement uses the IEEE 802.1ag CFM infrastructure.

Generally, Ethernet frame delay measurements are made in a peer fashion from one MEP or CFM session to another. However, these measurements are not made to maintenance association intermediate points (MIPs).

For a complete description of Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.

Types of Ethernet Frame Delay Measurements

There are two types of Ethernet frame delay measurements:

- One-way
- Two-way (round-trip)

For one-way Ethernet frame delay measurement, either MEP can send a request to begin a one-way delay measurement to its peer MEP. However, the statistics are collected only at the receiver MEP. This feature requires the clocks at the transmitting and receiving MEPs to be synchronized. If these clocks fall out of synchronization, only one-way delay variation and average delay variation values are computed correctly

(and will, therefore, be valid). Use the **show** commands at the receiver MEP to display one-way delay statistics.

For two-way (round-trip) Ethernet frame delay measurement, either MEP can send a request to begin a two-way delay measurement to its peer MEP, which responds with timestamp information. Run-time statistics are collected and displayed at the initiator MEP. The clocks do not need to be synchronized at the transmitting and receiving MEPs. Junos OS supports timestamps in delay measurement reply (DMR) frames to increase the accuracy of delay calculations.

Use the **show** commands at the initiator MEP to display two-way delay statistics, and at the receiver MEP to display one-way delay statistics.

You can create an iterator profile to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for delay measurement or loss measurement.

Limitations

The following are some limitations with regard to using Ethernet frame delay measurement:

- Ethernet frame delay measurements are available only when distributed periodic packet management (PPM) is enabled.
- The statistics collected are lost after a graceful Routing Engine switchover (GRES).
- You can monitor only one session to the same remote MEP or MAC address.
- Accuracy is compromised when the system configuration changes (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

RELATED DOCUMENTATION

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | **339**

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | **340**

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | **343**

Triggering an Ethernet Frame Delay Measurement Session on a Switch | **342**

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). By default, Ethernet frame delay measurement uses software for timestamping and delay calculations. You can configure an EX Series switch to perform and display Ethernet frame delay measurements on Ethernet interfaces. The switches support software-assisted timestamping.

Before you can begin configuring MEP interfaces to support Ethernet frame delay measurements on switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly
- Enabled distributed periodic packet management (PPM) (distributed PPM is enabled by default)

To configure MEP interfaces on switches to support Ethernet frame delay measurements:

1. Enable the Ethernet frame delay measurement by issuing the **monitor ethernet delay-measurement** operational mode command. In this command, you must specify one measurement type (either one-way or two-way measurement), and you must specify either the unicast MAC address of the peer MEP or its numeric identifier.

   Optionally, you can also specify the following parameters:

   - Number of frames to send to the peer MEP (**count *count***)
   - Number of seconds to wait between sending frames (**wait *time***)
   - Priority value of the delay measurement request frame (**priority *value***)
   - Size of the data in the data TLV of the request packet (**size *value***)
   - Suppression of the insertion of the session ID TLV in the request packet (**no-session-id-tlv**)

   ```
   user@switch> monitor ethernet delay-measurement maintenance-domain md-name
   maintenance-association ma-name one-way mep remote-mep-id count count wait
   time priority value size value no-session-id-tlv
   ```

RELATED DOCUMENTATION

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343

Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342

Understanding Ethernet Frame Delay Measurements on Switches | 336

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). You can configure the frame delay measurements in either a one-way mode or a two-way (round-trip) mode to gather frame delay statistics. For one-way Ethernet frame delay measurement, clocks at the local and remote MEPs need to be synchronized. However, clock synchronization is not required for two-way Ethernet frame delay measurement.

Before you begin configuring one-way Ethernet frame delay measurements on two EX Series switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly on both the switches
- Synchronized the system clocks of both the switches

To configure one-way Ethernet frame delay measurements:

1. Configure the maintenance domain, maintenance association, and MEP ID on both the switches.

2. From either switch, start a one-way Ethernet frame delay measurement:

   ```
   user@switch> monitor ethernet delay-measurement maintenance-domain md-name
   maintenance-association ma-name one-way mep remote-mep-id count count wait
   time
   ```

You can view the result on the other switch:

```
user@switch> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md-name maintenance-association ma-name local-mep mep-id
remote-mep mep-id
```

RELATED DOCUMENTATION

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343

Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342

Understanding Ethernet Frame Delay Measurements on Switches | 336

Configuring an Iterator Profile on a Switch (CLI Procedure)

Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor service-level agreements (SLAs). You can create an iterator profile with its parameters to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for two-way delay measurement.

To create an iterator profile:

1. Specify a name for an SLA iterator profile—for example, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@switch# edit sla-iterator-profiles i1
```

2. (Optional) Configure the cycle time, which is the time (in milliseconds) between back-to-back transmissions of SLA frames.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@switch# set cycle-time cycle-time-value
```

3. (Optional) Configure the iteration period, which indicates the maximum number of cycles per iteration (the number of connections registered to an iterator cannot exceed this value).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@switch# set iteration-period iteration-period-value
```

4. Configure the measurement type as two-way delay measurement.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@switch# set measurement-type two-way-delay
```

5. (Optional) Configure the calculation weight for delay.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@switch# set calculation-weight delay delay-value
```

6. (Optional) Configure the calculation weight for delay variation.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
  i1]
user@switch# set calculation-weight delay-variation delay-variation-value
```

7. Configure a remote MEP with the iterator profile.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
  maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@switch# set sla-iterator-profiles i1
```

RELATED DOCUMENTATION

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343
- Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342
- Understanding Ethernet Frame Delay Measurements on Switches | 336

Triggering an Ethernet Frame Delay Measurement Session on a Switch

To trigger Ethernet frame delay measurement, use the **monitor ethernet delay-measurement** operational command and specify the following values:

- Either one-way (**one-way**) or two-way (**two-way**) measurement
- Either the MAC address (**remote-mac-address**) or the MEP ID (**mep**) of the remote host
- The maintenance domain (**maintenance-domain**)

- The maintenance association (**maintenance-association**)
- (Optional) Any or all of these options: **count**, **size**, **wait**, no-session-id-tlv, **priority**

For example:

```
user@switch> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10 size 50 wait 5 no-session-id-tlv priority 1
```

RELATED DOCUMENTATION

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | **339**

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | **340**

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | **343**

Understanding Ethernet Frame Delay Measurements on Switches | **336**

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). You can configure the frame delay measurements in either a one-way mode or a two-way (round-trip) mode to gather frame delay statistics. For one-way Ethernet frame delay measurement, clocks at the local and remote MEPs need to be synchronized. However, clock synchronization is not required for two-way Ethernet frame delay measurement.

Before you begin configuring two-way Ethernet frame delay measurements on two EX Series switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly on both the switches

To configure two-way Ethernet frame delay measurements:

1. Configure the maintenance domain, maintenance association, and MEP ID on both the switches.

2. From either switch, start a two-way Ethernet frame delay measurement:

```
user@switch> monitor ethernet delay-measurement maintenance-domain md-name
maintenance-association ma-name two-way mep remote-mep-id count count wait
time
```

You can view the result on the other switch:

```
user@switch> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md-name maintenance-association ma-name local-mep mep-id
remote-mep mep-id
```

RELATED DOCUMENTATION

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340
- Triggering an Ethernet Frame Delay Measurement Session on a Switch | 342
- Understanding Ethernet Frame Delay Measurements on Switches | 336

CHAPTER 9

Ethernet OAM for Security Devices

IN THIS CHAPTER

- Configuring Ethernet OAM Connectivity Fault Management | 345
- Configuring Ethernet OAM Link Fault Management | 368

Configuring Ethernet OAM Connectivity Fault Management

IN THIS SECTION

- Understanding Ethernet OAM Connectivity Fault Management | 345
- Configuring the Continuity Check Protocol on a Security Device | 348
- Configuring the Link Trace Protocol on a Security Device | 350
- Creating a Maintenance Domain on a Security Device | 350
- Configuring a Maintenance Domain MIP Half Function on a Security Device | 352
- Creating a Maintenance Association on a Security Device | 352
- Configuring a Maintenance Association End Point on a Security Device | 353
- Example: Configuring Ethernet OAM Connectivity Fault Management on a Security Device | 355

Ethernet interfaces on SRX Series devices support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The 802.1ag is an IEEE standard for connectivity fault management (CFM). the below topics discuss the overview of CFM, configuration of continuity check protocol, link trace protocol, creating a maintenance domain, and configuration of Ethernet OAM CFM on a security device.

Understanding Ethernet OAM Connectivity Fault Management

Ethernet interfaces on SRX Series devices support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The 802.1ag is an IEEE standard for connectivity fault management (CFM). The IEEE 802.1ag provides a specification for Ethernet CFM. The Ethernet network can consist of one or more

service instances. A service instance could be a VLAN or a concatenation of VLANs. The goal of CFM is to provide a mechanism to monitor, locate, and isolate faulty links.

> **NOTE:** Support for the IEEE 802.1ag standard for OAM on SRX Series devices depends on the Junos OS release running on the device.

Starting in Junos OS Release 15.1X49-D80, Ethernet OAM CFM is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, Ethernet OAM CFM is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Ethernet OAM CFM is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

CFM support includes the following features:

- Fault monitoring using the Continuity Check Protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
- Path discovery and fault verification using the Link Trace protocol. This feature is not supported in Junos OS Release 12.3X48-D65.
- Fault isolation using the Loopback protocol.

  The Loopback protocol is used to check access to maintenance association end points (MEPs) under the same maintenance association (MA). The Loopback messages are triggered by an administrator using the **ping ethernet** command.

> **NOTE:** Virtual private LAN service (VPLS) is not supported on SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1400, and SRX1500 devices.

CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains. Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible.

In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought of as a full mesh of maintenance association end points (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages. There is also a maintenance association intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outer domains are assigned a higher level than the inner domains. You configure customer end points to have the highest maintenance domain level. The maintenance domain level is a mandatory parameter that indicates the nesting relationships between various maintenance domains. The level is embedded in each CFM frame. CFM messages within a given level are processed by MEPs at that same level.

To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and MEPs.

The limitations for CFM are as follows:

- You cannot configure MEP and MIP on the same VLAN.
- CFM and link fault management (LFM) can be configured on the same interface.
- You cannot configure CFM with Generic VLAN Registration Protocol (GVRP).
- CFM is not supported on VoIP VLAN ports.
- On SRX240, and SRX550M devices, the default Loopback message (LBM) packet size is 113 bytes.

Benefits of Ethernet CFM

Ethernet CFM provides the following benefits:

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers

CFM over VDSL and PPPoE interfaces for SRX210, SRX220, SRX240, SRX320, SRX340, SRX345, SRX380, SRX550, and SRX550M Devices

Starting in Junos OS Release 12.3X48-D65, on SRX210, SRX220, SRX240, and SRX550 devices, Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) is supported on very-high-bit-rate digital subscriber line (VDSL) and Point-to-Point Protocol over Ethernet (PPPoE) interfaces in addition to Ethernet interfaces.

CFM over VDSL should be configured on the pt interface. To support CFM over PPPoE, you need to configure maintenance domain and maintenance association end point (MEP). The CFM over VDSL interface supports down direction MEP, continuity check, and loopback protocols.

The following are the limitations when configuring Ethernet CFM over VDSL or Layer 3 interface:

- CFM action profiles are not supported on the Point-to-Point Protocol over Ethernet (PPPoE) logical interface on SRX210, SRX220, SRX240, SRX550, and SRX650 devices.
- Synthetic loss measurement on demand is supported only on SRX320, SRX340, SRX345, and SRX550M devices. Proactive synthetic loss measurement is not supported.

- When CFM over PPPoE is implemented, CFM must be applied on the PPPoE logical interface and not on the underlying interface.
- CFM over VDSL can be implemented as a MEP but not as a MIP.
- CFM higher-level pass-through over a VDSL or Gigabit Ethernet interface in Layer 3 interface mode is not supported.
- For a VLAN-tagged VDSL interface, CFM must always be applied on the respective logical interface and not over the physical interface.
- When CFM is enabled on VDSL, CFM packets are dropped randomly, causing CFM sessions to flap based on the timer when transit traffic exceeds the line rate. Flapping occurs because the VDSL Mini-Physical Interface Module (Mini-PIM) cannot differentiate and prioritize CFM packets.

Configuring the Continuity Check Protocol on a Security Device

The Continuity Check Protocol is used for fault detection by a maintenance association end point (MEP) within a maintenance association. The MEP periodically sends continuity check multicast messages. The receiving MEPs use the continuity check messages (CCMs) to build a MEP database of all MEPs in the maintenance association.

Starting in Junos OS Release 12.3X48-D65, on SRX210, SRX220, SRX240, and SRX550 devices, the continuity check protocol for Ethernet Operation, Administration, and Management (OAM) connectivity fault management is supported over VDSL and PPPoE interfaces in addition to Ethernet interfaces.

Starting in Junos OS Release 15.1X49-D80, the continuity check protocol for Ethernet OAM CFM is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, the continuity check protocol for Ethernet OAM CFMis supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

The continuity check protocol for Ethernet OAM CFM is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

To configure the Continuity Check Protocol:

1. Enable the Continuity Check Protocol.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
       maintenance-association ma-name]
   user@host# set continuity-check
   ```

2. Specify the continuity check hold interval. The hold interval is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes (not supported in Junos OS Release 12.3X48-D60).

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name continuity-check]
user@host# set hold-interval number
```

3. Specify the CCM interval. The interval is the time between the transmission of CCMs. You can specify 10 minutes (10m), 1 minute (1m), 10 seconds (10s), 1 second (1s), or 100 milliseconds (100ms).

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name continuity-check]
user@host# set interval number
```

4. Specify the number of CCMs (that is, protocol data units) that can be lost before the MEP is marked as down. The default number of protocol data units (PDUs) is 3.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name continuity-check]
user@host# set loss-threshold number
```

NOTE: If the CCM interval is 100 milliseconds, only four MEPs are supported on a device.

Configuring the Link Trace Protocol on a Security Device

Starting in Junos OS Release 15.1X49-D80, configuring the Link Trace protocol for Ethernet OAM connectivity fault management is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, configuring the Link Trace protocol for Ethernet OAM connectivity fault management is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Configuring the Link Trace protocol for Ethernet OAM connectivity fault management is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

The Link Trace protocol is used for path discovery between a pair of maintenance points. Link Trace Messages (LTMs) are triggered by an administrator using the **traceroute ethernet** command to verify the path between a pair of MEPs under the same maintenance association. LTMs can also be used to verify the path between a MEP and a MIP under the same maintenance domain.

To configure the Link Trace protocol:

1. Configure the Link Trace path age timer. If no response to a Link Trace request is received, the request and response entries are deleted after the age timer expires.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set linktrace age time
   ```

2. Configure the number of Link Trace Reply (LTR) entries to be stored per Link Trace request.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set linktrace path-database-size path-database-size
   ```

Creating a Maintenance Domain on a Security Device

A maintenance domain consists of network entities such as operators, providers, and customers. A maintenance domain is a management space for managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary. Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outer domains are assigned a higher level than the inner domains. You configure customer end points to have the highest maintenance domain level. The maintenance domain level is a mandatory parameter that indicates the nesting relationships between various maintenance domains.

To enable connectivity fault management (CFM) on an Ethernet interface, maintenance domains, maintenance associations, and maintenance association end points (MEPs) must be created and configured.

Starting in Junos OS Release 12.3X48-D65, on SRX210, SRX220, SRX240, and SRX550 devices, creating a maintenance domain for Ethernet OAM CFM is supported over VDSL and PPPoE interfaces in addition to Ethernet interfaces.

Starting in Junos OS Release 15.1X49-D80, creating a maintenance domain for Ethernet OAM CFM is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, creating a maintenance domain for Ethernet OAM CFM is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Creating a maintenance domain for Ethernet OAM CFM is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

To create a maintenance domain:

1. Specify a name for the maintenance domain.

   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set maintenance-domain *domain-name*

2. Specify a format for the maintenance domain name. If you do not specify a format, no name is configured.
   - A plain ASCII character string
   - A Domain Name System (DNS) format
   - A media access control (MAC) address plus a two-octet identifier in the range 0 through 65,535
   - None

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]
   user@host# set name-format *format*

   For example, to specify the name format as a MAC address plus a two-octet identifier:

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]

   user@host# set name-format *mac+2oct*

3. Configure the maintenance domain level, which is used to indicate the nesting relationship between this domain and other domains. Use a value from 0 through 7.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]

   user@host# set level *level-number*

Configuring a Maintenance Domain MIP Half Function on a Security Device

Starting in Junos OS Release 15.1X49-D80, configuring a maintenance domain MIP half function for Ethernet OAM connectivity fault management is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, configuring a maintenance domain MIP half function for Ethernet OAM connectivity fault management is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Configuring a maintenance domain MIP half function for Ethernet OAM connectivity fault management is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

MIP half function (MHF) divides the maintenance association intermediate point (MIP) functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loopback and Link Trace messages to help isolate faults. Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be the same.

To configure the MIP half function:

[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]
user@host# set mip-half-function *default*

NOTE:

- If SRX340, or SRX345 devices are configured as MIPs, ensure that a static MAC is configured in the Ethernet switching table with the next-hop interface to the MEP MAC.
- You cannot configure MIP in a nondefault domain.
- In Q-in-Q mode, double tag packets are not retained by MIP.
- A maximum of 116 MIPs can be configured on a device.

Creating a Maintenance Association on a Security Device

In a connectivity fault management (CFM) maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought of as a full mesh of maintenance association end points (MEPs) having similar characteristics.

Starting in Junos OS Release 12.3X48-D65, on SRX210, SRX220, SRX240, and SRX550 devices, creating a maintenance association for Ethernet OAM connectivity fault management is supported over VDSL and PPPoE interfaces in addition to Ethernet interfaces.

Starting in Junos OS Release 15.1X49-D80, creating a maintenance association for Ethernet OAM CFM is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, creating a maintenance association for Ethernet OAM CFM is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Creating a maintenance association for Ethernet OAM CFM is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

To create a maintenance association:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@host# set maintenance-association ma-name
```

NOTE: On SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX550M, and SRX650 devices, a maximum of seven maintenance associations are supported.

Configuring a Maintenance Association End Point on a Security Device

Starting in Junos OS Release 12.3X48-D65, on SRX210, SRX220, SRX240, and SRX550 devices, configuring a maintenance association end point for Ethernet OAM CFM is supported over VDSL and PPPoE interfaces in addition to Ethernet interfaces.

Starting in Junos OS Release 15.1X49-D80, configuring a maintenance association end point for Ethernet OAM CFM is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, configuring a maintenance association end point for Ethernet OAM CFM is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Configuring a maintenance association end point for Ethernet OAM CFM is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

To configure a MEP:

1. Specify an ID for the MEP. The value can be from 1 through 8191.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
      maintenance-association ma-name]
   user@host# set mep mep-id
   ```

2. Enable MEP automatic discovery if you want to have the MEP accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

3. Specify that CFM CCM packets be transmitted only in one direction for the MEP. That is, set the direction as down so that CCMs are transmitted only out of (not into) the interface configured on this MEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set direction down
```

4. Specify the logical interface to which the MEP is attached. It can be either an access interface or a trunk interface. If you specify a trunk interface, the VLAN associated with that interface must have a VLAN ID.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set interface interface-name
```

5. Configure a remote MEP from which CCMs are expected. If automatic discovery is not enabled, the remote MEP must be configured under the **mep** statement; otherwise, the CCMs from the remote MEP will be treated as errors.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
    maintenance-association ma-name mep mep-id]
user@host# set remote-mep mep-id
```

NOTE: You cannot configure MEPs at different levels for the same VLANs.

Example: Configuring Ethernet OAM Connectivity Fault Management on a Security Device

IN THIS SECTION

- Requirements | 355
- Overview | 355
- Configuring Ethernet OAM Connectivity Fault Management | 356
- Verification | 363

Starting in Junos OS Release 15.1X49-D80, Ethernet OAM connectivity fault management is supported on SRX1500 devices.

Starting in Junos OS Release 15.1X49-D75, Ethernet OAM connectivity fault management is supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Ethernet OAM connectivity fault management is not supported from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D70.

Connectivity Fault Management (CFM) provides a mechanism to monitor, locate, and isolate faulty links.

This example describes how to enable and configure an end-to-end OAM CFM session on an Ethernet interface.

Requirements

This example uses the following hardware and software components:

- Three SRX Series devices connected by a point-to-point Ethernet link.
- Junos OS Release 12.1X44-D10 or later for SRX Series devices.

Overview

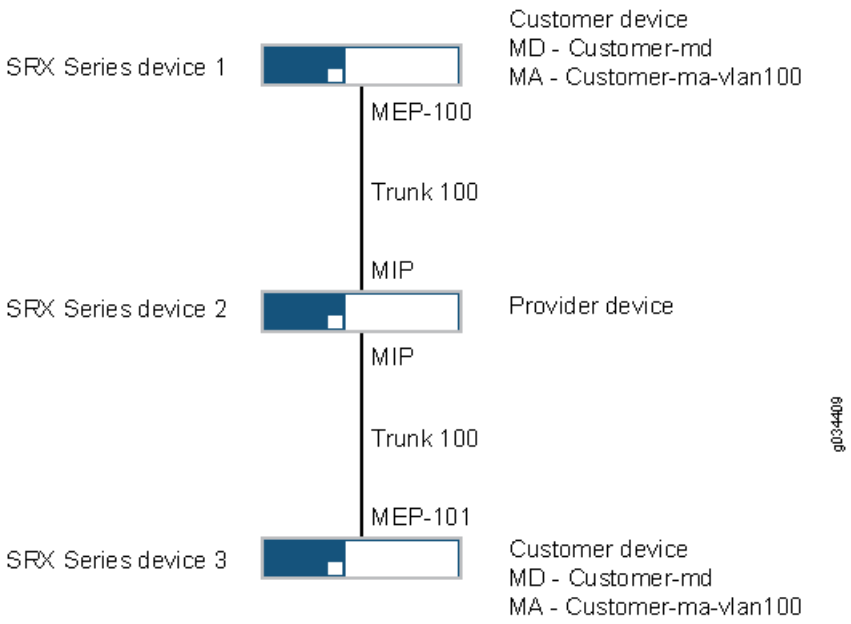
Ethernet interfaces on SRX Series devices support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides a specification for Ethernet connectivity fault management (CFM). CFM can be used to detect faults in the network path between the customer premises devices. It also helps in detecting the device or node in the provider network, where the failure occurred.

This example describes how to configure an end to end CFM session. In this example, three devices are connected by a point-to-point Ethernet link. The link between these devices is monitored using CFM. To check connectivity or fault through the provider network, maintenance intermediate point (MIP) is configured.

Topology

Figure 21 on page 356 shows three SRX Series devices connected by a point-to-point Ethernet link.

Figure 21: Ethernet CFM with SRX Series Devices



Legend
MA - Maintenance Association
MD - Maintenance Domain
MEP - Maintenance Association End Point
MIP - Maintenance Association Intermediate Point

Configuring Ethernet OAM Connectivity Fault Management

IN THIS SECTION

- Configuring Ethernet OAM Connectivity Fault Management on Device 1 | **356**
- Configuring Ethernet OAM CFM with MIP Half Function on Device 2 | **359**
- Configuring Ethernet OAM Connectivity Fault Management on Device 3 | **361**

Configuring Ethernet OAM Connectivity Fault Management on Device 1

CLI Quick Configuration

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

```
set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members v100
set vlans v100 vlan-id 100
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md level 5
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 100 interface ge-0/0/4.0
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 100 interface vlan 100
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 100 auto-discovery
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma continuity-check interval 10s
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma continuity-check hold-interval 20
```

Step-by-Step Procedure

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

To enable and configure OAM CFM on device 1:

1. Define a VLAN and enable the interface for family Ethernet switching with interface mode trunk or access.

   ```
   [edit]
   user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode trunk
   user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members v100
   user@host# set vlans v100 vlan-id 100
   ```

2. Specify the maintenance domain name and the maintenance domain level.

   ```
   [edit protocols oam ethernet connectivity-fault-management ]
   user@host# set maintenance-domain Customer-md level 5
   ```

3. Create a maintenance association and configure MEP.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md]
   user@host# set maintenance-association Customer-ma mep 100 interface ge-0/0/4.0
   ```

```
user@host# set maintenance-association Customer-ma mep 100 interface vlan 100
```

4. Enable MEP automatic discovery.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma]
user@host# set mep 100 auto-discovery
```

5. Enable the Continuity Check Protocol and specify the continuity check interval and hold interval.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma]
user@host# set continuity-check interval 10s
user@host# set continuity-check hold-interval 20
```

Results

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

For brevity, this **show protocols** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show protocols
```

```
oam {
   ethernet {
      connectivity-fault-management {
         maintenance-domain Customer-md {
            level 5;
            maintenance-association Customer-ma {
               continuity-check {
                  interval 10s;
                  hold-interval 20;
               }
               mep 100 {
                  interface ge-0/0/4.0 vlan 100;
                  auto-discovery;
               }
```

```
        }
      }
    }
  }
}
```

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

Configuring Ethernet OAM CFM with MIP Half Function on Device 2

CLI Quick Configuration

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

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members v100
set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members v100
set vlans v100 vlan-id 100
set protocols oam ethernet connectivity-fault-management maintenance-domain default-5 v100
set protocols oam ethernet connectivity-fault-management maintenance-domain default-5 mip-half-function
    default
```

Step-by-Step Procedure

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

To configure MIP half function:

1. Define a VLAN and enable the interface for family Ethernet switching with interface mode trunk or access.

   ```
   [edit]
   user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
   user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members v100
   user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode trunk
   user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members v100
   user@host# set vlans v100 vlan-id 100
   ```

2. Create a maintenance domain and configure VLAN.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   ```

```
user@host# set maintenance-domain default-5 v100
```

3. Create a MIP half function.

```
[edit protocols oam ethernet connectivity-fault-management ]
user@host# set maintenance-domain default-5 mip-half-function default
```

NOTE: If you want to configure traceoptions, run the following commands:

```
set protocols oam ethernet connectivity-fault-management traceoptions file CFM_trace
set protocols oam ethernet connectivity-fault-management traceoptions flag all
```

Results

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

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show protocols
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file CFM_trace;
                    flag all;
                }
                maintenance-domain default-5 {
                    v100;
                    mip-half-function default;
                }
            }
        }
    }
```

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

Configuring Ethernet OAM Connectivity Fault Management on Device 3

CLI Quick Configuration

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

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members v100
set vlans v100 vlan-id 100
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md level 5
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 101 interface ge-0/0/1.0
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 101 interface vlan 100
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma mep 101 auto-discovery
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma continuity-check hold-interval 20
set protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma continuity-check interval 10s
```

Step-by-Step Procedure

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

To enable and configure OAM CFM on Device 3:

1. Define a VLAN and enable the interface for family Ethernet switching with interface mode trunk or access.

   ```
   [edit]
   user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
   user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members v100
   user@host# set vlans v100 vlan-id 100
   ```

2. Specify the maintenance domain name and the maintenance domain level.

   ```
   [edit protocols oam ethernet connectivity-fault-management ]
   user@host# set maintenance-domain Customer-md level 5
   ```

3. Create a maintenance association and configure MEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md]
user@host# set maintenance-association Customer-ma mep 101 interface ge-0/0/1.0
user@host# set maintenance-association Customer-ma mep 101 interface vlan 100
```

4. Enable MEP automatic discovery.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md]
user@host# set maintenance-association Customer-ma mep 101 auto-discovery
```

5. Enable the Continuity Check Protocol and specify the continuity check interval and hold interval.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain Customer-md
   maintenance-association Customer-ma]
user@host# set continuity-check interval 10s
user@host# set continuity-check hold-interval 20
```

Results

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

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show protocols
   oam {
      ethernet {
         connectivity-fault-management {
            maintenance-domain Customer-md {
               level 5;
               maintenance-association Customer-ma {
                  continuity-check {
                     interval 10s;
                     hold-interval 20;
                  }
                  mep 101 {
                     interface ge-0/0/1.0 vlan 100;
                     auto-discovery;
                  }
               }
```

```
        }
      }
    }
  }
```

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

Verification

IN THIS SECTION

- Verifying the OAM CFM Configuration on Device 1 | **363**
- Verifying the OAM CFM Configuration with MIP Half Function on Device 2 | **365**
- Verifying the OAM CFM Configuration on Device 3 | **365**
- Verifying the Path Using the Link Trace Protocol | **367**
- Verifying MEP Continuity Using Ping | **367**

Confirm that the configuration is working properly.

Verifying the OAM CFM Configuration on Device 1

Purpose

Verify that OAM CFM has been configured properly.

Action

From operational mode, enter the following commands:

- **show oam ethernet connectivity-fault-management adjacencies** to display connectivity-fault-management adjacencies.
- **show oam ethernet connectivity-fault-management interfaces** to display the Ethernet OAM information for the specified interface.

These commands produce the following sample output:

`user@host#` **show oam ethernet connectivity-fault-management adjacencies**

```
Mep-id   Interface          State              Timer to Expire
          101     ge-0/0/4.0         ok                 29
```

`user@host#` **show oam ethernet connectivity-fault-management interfaces**

```
Interface         Link      Status       Level  MEP         Neighbours
                                                           Identifier
       ge-0/0/4.0          Up        Active       5      100         1
```

user@host# **show oam ethernet connectivity-fault-management interfaces detail**

```
Interface name: ge-0/0/4.0, vlan 100, Interface status: Active, Link status: Up
  Maintenance domain name: Customer-md, Format: string, Level: 5
    Maintenance association name: Customer-ma, Format: string
    Continuity-check status: enabled, Interval: 10s
    MEP identifier: 100, Direction: down, MAC address: 2c:6b:f5:62:29:84
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : no
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : no
    Statistics:
      CCMs sent                                     : 7
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 0
      1DMs sent                                     : 0
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0
    Remote MEP count: 1
      Identifier    MAC address        State    Interface
        101     80:71:1f:ad:53:81       ok    ge-0/0/4.0
```

Meaning

- If the **show oam ethernet connectivity-fault-management interfaces detail** command output displays continuity-check status as **enabled** and displays details of the remote MEP, it means that connectivity fault management (CFM) was configured properly.
- If the **show oam ethernet connectivity-fault-management adjacencies** command output displays the state as **ok**, it indicates that the Continuity Check Protocol is up.

Verifying the OAM CFM Configuration with MIP Half Function on Device 2

Purpose

Verify that OAM CFM has been configured properly.

Action

From operational mode, run the **show oam ethernet connectivity-fault-management mip** command.

```
user@host# show oam ethernet connectivity-fault-management mip vlan 100
```

```
default maintenance-domain mhf    : default

  Interface       Level
  ge-0/0/1.0          5
  ge-0/0/4.0          5
```

Meaning

The **show oam ethernet connectivity-fault-management mip** command output displays the MIP information.

Verifying the OAM CFM Configuration on Device 3

Purpose

Verify that OAM CFM has been configured properly.

Action

From operational mode, enter the following commands:

- **show oam ethernet connectivity-fault-management adjacencies** to display connectivity-fault-management adjacencies.
- **show oam ethernet connectivity-fault-management interfaces** to display the Ethernet OAM information for the specified interface.

```
user@host# show oam ethernet connectivity-fault-management adjacencies
```

```
Mep-id      Interface          State       Timer to Expire
          100       ge-0/0/1.0         ok            27
```

user@host# **show oam ethernet connectivity-fault-management interfaces detail**

```
Interface name: ge-0/0/1.0, vlan 100, Interface status: Active, Link status: Up
  Maintenance domain name: Customer-md, Format: string, Level: 5
    Maintenance association name: Customer-ma, Format: string
    Continuity-check status: enabled, Interval: 10s
    MEP identifier: 101, Direction: down, MAC address: 80:71:1f:ad:53:81
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : no
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : no
    Statistics:
      CCMs sent                                     : 77
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 0
      1DMs sent                                     : 0
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0
    Remote MEP count: 1
      Identifier    MAC address        State    Interface
        100     2c:6b:f5:62:29:84       ok    ge-0/0/1.0
```

Meaning

- If the **show oam ethernet connectivity-fault-management interfaces detail** command output displays continuity-check status as **enabled** and displays details of the remote MEP, it means that connectivity fault management (CFM) was configured properly.
- If the **show oam ethernet connectivity-fault-management adjacencies** command output displays the state as **ok**, it indicates that the Continuity Check Protocol is up.

Verifying the Path Using the Link Trace Protocol

Purpose

Verify the path between maintenance endpoints.

Action

From operational mode, enter the **traceroute ethernet** command.

`user@host#` **traceroute ethernet maintenance-domain Customer-md maintenance-association Customer-ma mep 101**

```
Linktrace to 80:71:1f:ad:53:81, Interface : ge-0/0/4.0
      Maintenance Domain: Customer-md, Level: 5
      Maintenance Association: Customer-ma, Local Mep: 100
      Transaction Identifier: 3
    Hop   TTL    Source MAC address        Next-hop MAC address
    .
    1     63     80:71:1f:ad:50:01         80:71:1f:ad:50:01
    2     62     80:71:1f:ad:53:81         00:00:00:00:00:00
```

Verifying MEP Continuity Using Ping

Purpose

Verify access to MEPs under the same maintenance association.

Action

From operational mode, enter the **ping ethernet** command.

`user@host#` **ping ethernet maintenance-domain Customer-md maintenance-association Customer-ma mep 101**

```
PING to 80:71:1f:ad:53:81, Interface ge-0/0/4.0
60 bytes from 80:71:1f:ad:53:81: lbm_seq=0
60 bytes from 80:71:1f:ad:53:81: lbm_seq=1
60 bytes from 80:71:1f:ad:53:81: lbm_seq=2
60 bytes from 80:71:1f:ad:53:81: lbm_seq=3
```

```
--- ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Configuring Ethernet OAM Link Fault Management

IN THIS SECTION

- Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways | **368**
- Example: Configuring Ethernet OAM Link Fault Management on a Security Device | **370**
- Example: Configuring Remote Loopback Mode on VDSL Interfaces on a Security Device | **375**

The Ethernet interfaces on SRX Series devices support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM). The below topics discuss the overview of Ethernet OAM LFM for SRX series devices, and examples of configuring OAM.

Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways

Starting in Junos OS Release 15.1X49-D70, Ethernet OAM link fault management for SRX Series services gateways is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

The Ethernet interfaces on SRX Series devices support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward-compatible with existing Ethernet technology.

The following OAM LFM features are supported:

- Discovery and link monitoring—The discovery process is triggered automatically when OAM is enabled on the interface. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard. 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. After the discovery process has been initiated, both sides

participate in discovery. The device performs link monitoring by sending periodic OAM protocol data units (PDUs) to advertise OAM mode, configuration, and capabilities.

You can specify the number of OAM PDUs that an interface can miss before the link between peers is considered down.

- Remote fault detection—Remote fault detection uses flags and events. Flags convey Link Fault (a loss of signal), Dying Gasp (an unrecoverable condition such as a power failure), and Critical Event (an unspecified vendor-specific critical event). You can specify the periodic OAM PDU sending interval for fault detection. SRX Series devices use the Event Notification OAM PDU to notify the remote OAM device when a problem is detected. You can specify the action to be taken by the system when the configured link-fault event occurs.
- Remote loopback—Remote loopback mode ensures link quality between the device and a remote peer during installation or troubleshooting. In this mode, when the interface receives a frame that is not an OAM PDU or a pause frame, it sends it back on the same interface on which it was received. The link appears to be in the active state. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.

  Junos OS can place a remote data terminal equipment (DTE) into loopback mode (if remote loopback mode is supported by the remote DTE). When you place a remote DTE into loopback mode, the interface receives the remote loopback request and puts the interface into remote loopback mode. When the interface is in remote loopback mode, all frames except OAM PDUs are looped back without any changes made to the frames. OAM PDUs continue to be sent and processed.

Table 27 on page 369 lists the interfaces modes supported.

Table 27: Supported Interface Modes

Interfaces	Mode
Physical interface (fe/ge)	Family • ccc • ethernet-switching • inet6 • inet • iso • mpls • tcc
	IFD encapsulations • ethernet-ccc • extended-vlan-ccc (IFD vlan-tagging mode) • ethernet-tcc • extended-vlan-tcc

Table 27: Supported Interface Modes *(continued)*

Interfaces	Mode
Aggregated Ethernet interface (Static or LACP lag)	Family • ethernet-switching • inet • mpls • iso • inet6
	IFD encapsulations • ethernet-ccc • extended-vlan-ccc (IFD vlan-tagging mode) • vlan-ccc

Example: Configuring Ethernet OAM Link Fault Management on a Security Device

IN THIS SECTION

- Requirements | 371
- Overview | 371
- Configuration | 372
- Verification | 374

Starting in Junos OS Release 15.1X49-D70, configuring Ethernet OAM link fault management is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

The Ethernet interfaces on the SRX Series devices support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example describes how to enable and configure OAM LFM on a Gigabit Ethernet or Fast Ethernet interface:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.1 R2 or later for SRX Series Services Gateways
- Any two models of SRX Series devices connected directly

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces as necessary. See *Example: Creating an Ethernet Interface*.
- Ensure that you configure the interfaces as per the interface modules listed in "Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways" on page 368

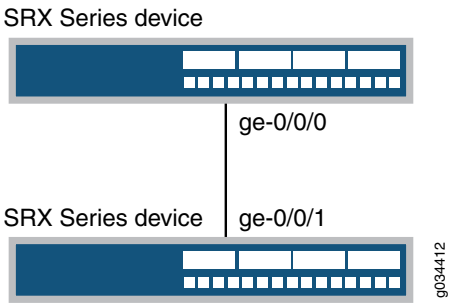
Overview

The Ethernet interfaces on the SRX Series devices support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example uses two SRX Series devices connected directly. Before you begin configuring Ethernet OAM LFM on these two devices, connect the two devices directly through supported interfaces. See "Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways" on page 368.

Figure 22 on page 371 shows the topology used in this example.

Figure 22: Ethernet LFM with SRX Series Devices



NOTE: For more information about configuring Ethernet OAM Link Fault Management, see Junos® OS Ethernet Interfaces.

Configuration

IN THIS SECTION

- Configuring Ethernet OAM Link Fault Management on Device 1 | **372**
- Configuring Ethernet OAM Link Fault Management on Device 2 | **373**

To configure Ethernet OAM LFM, perform these tasks:

Configuring Ethernet OAM Link Fault Management on Device 1

CLI Quick Configuration

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

```
set protocols oam ethernet link-fault-management interface ge-0/0/0
set protocols oam ethernet link-fault-management interface ge-0/0/0 pdu-interval 800
set protocols oam ethernet link-fault-management interface ge-0/0/0 link-discovery active
```

Step-by-Step Procedure

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

To configure Ethernet OAM LFM on device 1:

1. Enable IEEE 802.3ah OAM support.

```
[edit protocols oam ethernet link-fault-management]
user@device1# set interface ge-0/0/0
```

2. Set the periodic OAM PDU-sending interval (in milliseconds) for fault detection.

```
[edit protocols oam ethernet link-fault-management]
user@device1# set interface pdu-interval 800
```

3. Specify that the interface initiates the discovery process.

```
[edit protocols oam ethernet link-fault-management]
```

```
user@device1# set interface ge-0/0/0 link-discovery active
```

Results

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

```
[edit]
user@device1# show protocols
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/0 {
                    pdu-interval 800;
                    link-discovery active;
                }
            }
        }
    }
}
```

Configuring Ethernet OAM Link Fault Management on Device 2

CLI Quick Configuration

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

```
set protocols oam ethernet link-fault-management interface ge-0/0/1
set protocols oam ethernet link-fault-management interface ge-0/0/1 pdu-interval 800
set protocols oam ethernet link-fault-management interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Step-by-Step Procedure

To configure Ethernet OAM LFM on device 2:

1. Enable OAM on the peer interface.

```
[edit protocols oam ethernet link-fault-management]
user@device2# set interface ge-0/0/1
```

2. Set the periodic OAM PDU-sending interval (in milliseconds) for fault detection.

```
[edit protocols oam ethernet link-fault-management]
user@device2# set interface ge-0/0/1 pdu-interval 800
```

3. Enable remote loopback support for the local interface.

```
[edit protocols oam ethernet link-fault-management]
user@device2# set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Results

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

```
[edit]
user@device2# show protocols
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/1 {
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
}
```

Verification

Verify the OAM LFM Configuration

Purpose

Verify that OAM LFM is configured properly.

Action

From operational mode, enter the **show oam ethernet link-fault-management** command.

```
user@device1> show oam ethernet link-fault-management
```

```
Interface: ge-0/0/0.0
Status: Running, Discovery state: Send Any
Peer address: 2001:bd8:00:31
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote entity information:
Remote MUX action: forwarding, Remote parser action: forwarding
Discovery mode: active, Unidirectional mode: unsupported
Remote loopback mode: supported, Link events: supported
Variable requests: unsupported
```

Meaning

The output displays the MAC address and the discovery state is **Send Any** if OAM LFM has been configured properly.

Example: Configuring Remote Loopback Mode on VDSL Interfaces on a Security Device

IN THIS SECTION

- Requirements | **376**
- Overview | **376**
- Configuration for Scenario 1 | **376**
- Configuration for Scenario 2 | **378**
- Verification | **379**

Starting in Junos OS Release 15.1X49-D110, configuring remote loopback mode in Ethernet OAM link fault management (LFM) on a VDSL interface is supported on SRX320, SRX340, SRX345, and SRX550M devices.

This example describes the following configuration scenarios:

Starting in Junos OS Release 12.3X48-D65, configuring remote loopback mode in Ethernet OAM link fault management (LFM) on a VDSL interface is supported on SRX210, SRX220, SRX240, and SRX550 devices.

This example describes the following configuration scenarios:

- Scenario 1: Configuring remote loopback mode on a VDSL interface.

- Scenario 2: Configuring remote loopback mode on a VDSL interface acting as a PPPOE's underlying interface.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 15.1X49-D110 or later for SRX Series Services Gateways
- An SRX 210/220/240/320/340/345/550/550M device connected with a DSLAM

Before you begin:

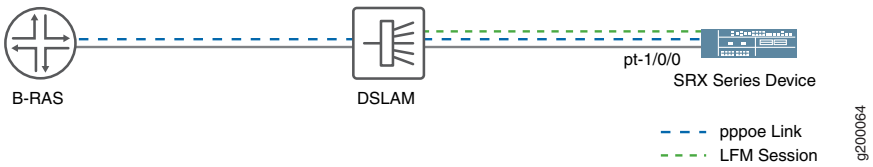
- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces as necessary. See *Example: Configuring VDSL2 Interfaces (Basic)*.
- Ensure that you configure the interfaces as per the interface modules listed in "Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways" on page 368
- Ensure that you configure PPPOE as per the instructions listed in *Example: Configuring PPPoE Interfaces*

Overview

This example uses an SRX Series device connected to a DSLAM. Before you begin configuring Ethernet OAM LFM on these two devices, connect the two devices directly through supported interfaces. See "Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways" on page 368.

Figure 23 on page 376 shows the topology used in this example.

Figure 23: Ethernet LFM with SRX Series Devices



NOTE: For more information about configuring Ethernet OAM Link Fault Management, see Junos® OS Ethernet Interfaces.

Configuration for Scenario 1

IN THIS SECTION

- Configuring Remote Loopback Mode on a VDSL interface of an SRX Series Device | 377

To configure remote loopback mode on a VDSL interface, perform these tasks:

Configuring Remote Loopback Mode on a VDSL interface of an SRX Series Device

CLI Quick Configuration

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

```
set protocols oam ethernet link-fault-management interface pt-1/0/0
set protocols oam ethernet link-fault-management interface pt-1/0/0 negotiation-options allow-remote-loopback
```

Step-by-Step Procedure

To configure remote loopback mode on a VDSL interface of an SRX Series device:

1. Enable OAM on a VDSL interface.

```
[edit protocols oam ethernet link-fault-management]
user@device2# set interface pt-1/0/0
```

2. Enable remote loopback support for the interface.

```
[edit protocols oam ethernet link-fault-management]
user@device2# set interface pt-1/0/0 negotiation-options allow-remote-loopback
```

Results

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

```
[edit]
user@device2# show protocols
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface pt-1/0/0 {
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
```

```
    }
  }
}
```

Configuration for Scenario 2

IN THIS SECTION

- Configuring Remote Loopback Mode on a PPPOE's underlying interface | 378

To configure remote loopback mode on a PPPOE's underlying interface, perform these tasks:

Configuring Remote Loopback Mode on a PPPOE's underlying interface

CLI Quick Configuration

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

```
set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0
set protocols oam ethernet link-fault-management interface pt-1/0/0 link-discovery active
set protocols oam ethernet link-fault-management interface pt-1/0/0 negotiation-options allow-remote-loopback
```

Step-by-Step Procedure

To configure remote loopback mode on a PPPOE's underlying interface:

1. Create the PPPoE interface pp0 and specify the logical PT interface pt-1/0/0 as the underlying interface.

   ```
   [edit protocols oam ethernet link-fault-management]
   user@device2# set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0
   ```

2. Specify that the interface initiates the discovery process.

   ```
   user@device2# set protocols oam ethernet link-fault-management interface pt-1/0/0 link-discovery active
   ```

3. Enable remote loopback mode.

```
user@device2# set protocols oam ethernet link-fault-management interface pt-1/0/0 negotiation-options
  allow-remote-loopback
```

Results

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

```
[edit]
user@device2# show protocols
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface pt-1/0/0 {
                    link-discovery active;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
}
```

Verification

Verify the OAM LFM Configuration

Purpose

Verify that OAM LFM is configured properly.

Action

From operational mode, enter the **show oam ethernet link-fault-management** command.

```
user@device1> show oam ethernet link-fault-management
```

```
Interface: pt-1/0/0.0
Status: Running, Discovery state: Send Any
Transmit interval: 300ms, PDU threshold: 3 frames, Hold time: 900ms
Peer address: 2001:db8:e5:b9:c8:ed
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
```

```
Loopback tracking: Disabled, Loop status: Unknown
Remote entity information:
Remote MUX action: forwarding, Remote parser action: forwarding
Discovery mode: active, Unidirectional mode: unsupported
Remote loopback mode: unsupported, Link events: supported
Variable requests: unsupported
```

Meaning

The output displays the MAC address and the discovery state is **Send Any** if OAM LFM has been configured properly.

3

PART

Uplink Failure Detection

Uplink Failure Detection Overview | 382

Configuring Uplink Failure Detection | 385

CHAPTER 10

Uplink Failure Detection Overview

IN THIS CHAPTER

- Understanding Uplink Failure Detection | 382

Understanding Uplink Failure Detection

IN THIS SECTION

- Uplink Failure Detection Overview | 382
- Failure Detection Pair | 384

Uplink failure detection allows Juniper Networks EX Series Ethernet Switches to detect link failure on uplink interfaces and to propagate the failure to the downlink interfaces so that servers connected to those downlink interfaces can switch over to secondary interfaces.

Uplink failure detection supports network adapter teaming and provides network redundancy. In network adapter teaming, all the network interface cards (NICs) on a server are configured in a primary or secondary relationship and share the same IP address. When the primary link goes down, the server transparently shifts the connection to the secondary link. With uplink failure detection, the switch monitors uplink interfaces for link failures. When it detects a failure, it disables the downlink interfaces. When the server detects disabled downlink interfaces, it switches over to the secondary link to help ensure balanced traffic flow on switches.

This topic describes:

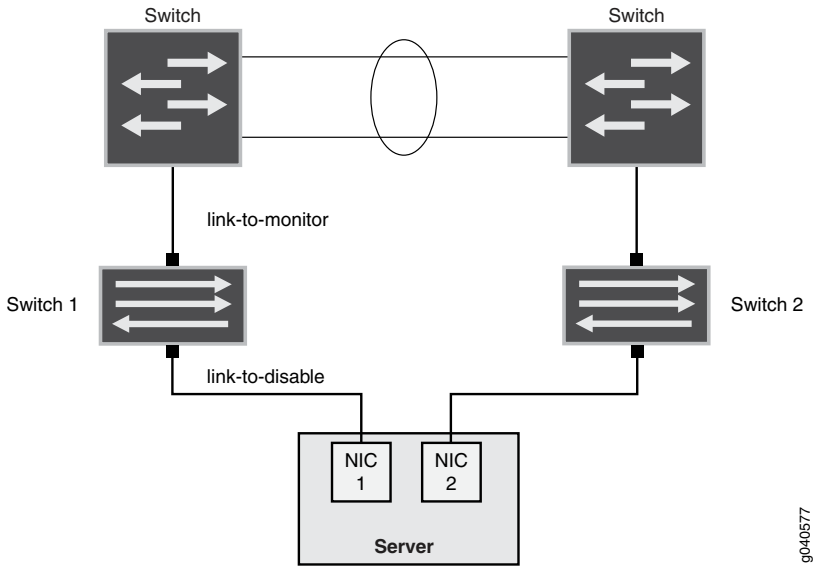
Uplink Failure Detection Overview

Uplink failure detection allows switches to monitor uplink interfaces to spot link failures. When a switch detects a link failure, it automatically disables the downlink interfaces in that group. The server that is

connected to the disabled downlink interfaces triggers a network-adapter failover to a secondary link to avoid any information drop.

Figure 24 on page 383 illustrates a typical setup for uplink failure detection.

Figure 24: Uplink Failure Detection Configuration on Switches



For uplink failure detection, you specify a group of uplink interfaces to be monitored and downlink interfaces to be brought down when an uplink fails. The downlink interfaces are bound to the uplink interfaces within the group. If all uplink interfaces in a group go down, then the switch brings down all downlink interfaces within that group. If any uplink interface returns to service, then the switch brings all downlink interfaces in that group back to service.

NOTE: Routed VLAN interfaces (RVIs) cannot be configured as uplink interfaces to be monitored.

The switch can monitor both physical-interface links and logical-interface links for uplink failures, but you must put the two types of interfaces in separate groups.

NOTE: To detect failure of logical interfaces, the server must run some high level protocol such as keepalives between the switch and the server.

Failure Detection Pair

Uplink failure detection requires that you create groups that contain uplink interfaces and downlink interfaces. Each group includes one of each of the following:

- A link-to-monitor interface—The link-to-monitor interfaces specify the uplink interfaces the switch monitors. You can configure a maximum of 48 uplink interfaces as link-to-monitor in a group.
- A link-to-disable interface—The link-to-disable interfaces specify the downlink interfaces the switch disables when the switch detects an uplink failure. You can configure a maximum of 48 downlink interfaces as link-to-disable in a group.

The link-to-disable interfaces are bound to the link-to-monitor interfaces within the group. When a link-to-monitor interface returns to service, the switch automatically enables all link-to-disable interfaces in the group.

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

CHAPTER 11

Configuring Uplink Failure Detection

IN THIS CHAPTER

- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385
- Verifying That Uplink Failure Detection Is Working Correctly | 386

Configuring Interfaces for Uplink Failure Detection (CLI Procedure)

You can configure uplink failure detection on EX Series switches to help ensure balanced traffic flow. Using this feature, switches can monitor and detect link failure on uplink interfaces and can propagate the failure to downlink interfaces so that servers connected to those downlink interfaces can switch over to secondary interfaces.

Follow these configuration guidelines:

- You can configure a maximum of 48 groups for each switch.
- You can configure a maximum of 48 uplink interfaces and 48 downlink interfaces in each group.
- You can configure physical links and logical links in separate groups.
- Ensure that all the interfaces in the group are up. If the interfaces are down, uplink failure detection does not work.

> **NOTE:** Routed VLAN interfaces (RVIs) cannot be configured as uplink interfaces to be monitored.

To configure uplink failure detection on a switch:

1. Specify a name for the group:

```
[edit protocols]
user@switch# set uplink-failure-detection group group-name
```

2. Add an uplink interface to the group:

```
[edit protocols]
```

```
user@switch# set uplink-failure-detection group group-name link-to-monitor interface-name
```

3. Repeat Step 2 for adding each uplink interface to the group.

> **NOTE:** An interface can be configured as link-to-monitor in multiple groups.

4. Add a downlink interface to the group:

```
[edit protocols]
user@switch# set uplink-failure-detection group group-name link-to-disable interface-name
```

5. Repeat Step 4 for adding each downlink interface to the group.

> **NOTE:** After you have configured a group, use the **show uplink-failure-detection group *group-name*** command to verify that all interfaces in the group are up.

RELATED DOCUMENTATION

Verifying That Uplink Failure Detection Is Working Correctly | 386

Understanding Uplink Failure Detection | 382

Verifying That Uplink Failure Detection Is Working Correctly

Purpose

Verify that the switch disables the downlink interface when it detects an uplink failure.

Action

1. View the current uplink-failure-detection status:

   ```
   user@switch> show uplink-failure-detection
   ```

   ```
   Group                     : group1
   Uplink                    :  ge-0/0/0*
   Downlink                  :  ge-0/0/1*
   Failure Action            :  Inactive
   ```

   NOTE: The asterisk (*) indicates that the link is up.

2. Disable the uplink interface:

   ```
   [edit]
   user@switch# set interface ge-0/0/0 disable
   ```

3. Save the configuration on the switch.

4. View the current uplink-failure-detection status:

   ```
   user@switch> show uplink-failure-detection
   ```

   ```
   Group                     : group1
   Uplink                    :  ge-0/0/0
   Downlink                  :  ge-0/0/1
   Failure Action            :  Active
   ```

Meaning

The output in Step 1 shows that the uplink interface is up, and hence that the downlink interface is also up, and that the status of **Failure Action** is **Inactive**.

The output in Step 4 shows that both the uplink and downlink interfaces are down and that the status of **Failure Action** is changed to **Active**. This output shows that uplink failure detection is working.

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

Understanding Uplink Failure Detection | 382

PART 4

Network Monitoring Using SNMP

SNMP Overview | **389**

SNMP MIBs and Traps Supported by Junos OS | **436**

Configuring Basic SNMP | **544**

Configuring SNMPv3 | **656**

Configuring SNMP for Routing Instances | **710**

Configuring SNMP Remote Operations | **734**

Tracing SNMP Activity | **758**

CHAPTER 12

SNMP Overview

IN THIS CHAPTER

- Understanding SNMP Implementation in Junos OS | 389
- SNMPv3 Overview | 395
- SNMPv3 Overview (QFX in Standalone Mode) | 396
- Loading MIB Files to a Network Management System | 397
- show snmp | 399
- Junos OS SNMP FAQ Overview | 401
- Junos OS SNMP FAQs | 402
- Managing Traps and Informs | 432

Understanding SNMP Implementation in Junos OS

IN THIS SECTION

- SNMP Architecture | 390
- SNMP on Junos OS | 392

SNMP enables the monitoring of network devices from a central location. This topic provides an overview of SNMP and describes how SNMP is implemented in the Junos OS.

This topic includes the following sections:

SNMP Architecture

IN THIS SECTION

- SNMP MIBs | 390
- SNMP Manager and Agent Authentication and Communication | 391
- SNMP Traps and Informs | 391

A typical SNMP implementation includes three components:

- Network management system (NMS)—A combination of hardware (devices) and software (the SNMP manager) that is used to monitor and administer a network. The manager polls the devices on your network how ever often you specify for information about network connectivity, activity, and events.
- Managed device—A managed device (also called a network element) is any device on a network that is managed by the NMS. Routers and switches are common examples of managed devices.
- SNMP agent—The SNMP agent is the SNMP process that resides on the managed device and communicates with the NMS. The SNMP agent exchanges network management information with the SNMP manager software running on an NMS, or host. The agent responds to requests for information and actions from the manager. The agent also controls access to the agent's MIB, the collection of objects that can be viewed or changed by the SNMP manager.

This topic contains the following sections:

SNMP MIBs

SNMP data is stored in a highly structured, hierarchical format known as a management information base (MIB). A MIB defines managed objects in a network device.

The MIB structure is based on a tree structure and defines a grouping of objects into related sets. Each object in the MIB is associated with an object identifier (OID), which names the object. The "leaf" in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs in your network device.

MIBs are either standard or enterprise-specific. Standard MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Depending on the vendor, many standard MIBs are delivered with the NMS software. You can also download the standard MIBs from the IETF website, www.ietf.org, and compile them into your NMS, if necessary.

For a list of standard supported MIBs, see "Standard SNMP MIBs Supported by Junos OS" on page 452.

Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific MIBs, you must obtain them from the manufacturer and compile them into your network management software.

For a list of Juniper Networks enterprise-specific supported MIBs, see "Enterprise-Specific SNMP MIBs Supported by Junos OS" on page 436.

SNMP Manager and Agent Authentication and Communication

SNMP uses a very basic form of authentication called community strings to control access between a manager and remote agents. Community strings are administrative names used to group collections of devices (and the agents running on them) into common management domains. If a manager and an agent share the same community, they can talk to one another. Many people associate SNMP community strings with passwords and keys because the jobs they do are similar. As a result, SNMP communities are traditionally referred to as strings.

Communication between the agent and the manager occurs in one of the following forms:

- **Get**, **GetBulk**, and **GetNext** requests—The manager requests information from the agent; the agent returns the information in a **Get** response message.
- **Set** requests—The manager changes the value of a MIB object controlled by the agent; the agent indicates status in a **Set** response message.
- **Traps** notification—The agent sends traps to notify the manager of significant events that occur on the network device.

SNMP Traps and Informs

Routers can send notifications to SNMP managers when significant events occur on a network device, most often errors or failures. SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The standard traps are compiled into the network management software. You can also download the standard traps from the IETF website, www.ietf.org.

For more information about standard traps supported by the Junos OS, see Standard SNMP Traps Supported on Devices Running Junos OS.

Enterprise-specific traps are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific traps, you must obtain them from the manufacturer and compile them into your network management software.

For more information about enterprise-specific traps supported by the Junos OS, see "Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500. For information about system logging severity levels for SNMP traps, see "System Logging Severity Levels for SNMP Traps" on page 393.

With traps, the receiver does not send any acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. An SNMP manager that receives an inform acknowledges the message with a response. For information about SNMP informs, see "Configuring SNMP Informs" on page 692.

SNMP on Junos OS

IN THIS SECTION

- Junos OS Support of SNMP Versions | **393**
- System Logging Severity Levels for SNMP Traps | **393**
- SNMP Communication Flow | **393**
- Trap Queuing | **394**

On Junos OS, SNMP uses both standard (developed by IETF and documented in RFCs) and Juniper Networks enterprise-specific MIBs.

> **NOTE:** By default, SNMP is not enabled on devices running Junos OS.

In Junos OS, the processes that maintain the SNMP management data include the following:

- A master SNMP agent which resides on the managed device and is managed by the NMS, or host.

  The Junos OS SNMP agent software consists of an SNMP master agent (known as the SNMP process, or snmpd). It resides on the managed device and is managed by the NMS, or host.

- Various subagents that reside on different modules of Junos OS, such as the Routing Engine. The master SNMP agent delegates all SNMP requests to the subagents. Each subagent is responsible for the support of a specific set of MIBs.

- Junos OS processes that share data with the subagents when polled for SNMP data (for example, interface-related MIBs).

The community string is the first level of management authentication implemented by the SNMP agent in Junos OS.

See the following sections for more information.

Junos OS Support of SNMP Versions

The Junos OS supports the following versions of SNMP:

- SNMPv1—The initial implementation of SNMP that defines the architecture and framework for SNMP.
- SNMPv2c—The revised protocol, with improvements to performance and manager-to-manager communications. Specifically, SNMPv2c implements community strings, which act as passwords when determining who, what, and how the SNMP clients can access the data in the SNMP agent. The community string is contained in SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests. The agent might require a different community string for **Get**, **GetBulk**, and **GetNext** requests (**read-only** access) than it does for **Set** requests (**read-write** access).
- SNMPv3—The most up-to-date protocol focuses on security. SNMPv3 defines a security model, user-based security model (USM), and a view-based access control model (VACM). SNMPv3 USM provides data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload. SNMPv3 VACM provides access control to determine whether a specific type of access (read or write) to the management information is allowed.

In addition, the Junos OS SNMP agent software accepts IPv4 and IPv6 addresses for transport over IPv4 and IPv6. For IPv6, the Junos OS supports the following features:

- SNMP data over IPv6 networks
- IPv6-specific MIB data
- SNMP agents for IPv6

System Logging Severity Levels for SNMP Traps

For some traps, when a trap condition occurs, regardless of whether the SNMP agent sends a trap to an NMS, the trap is logged if the system logging is configured to log an event with that system logging severity level.

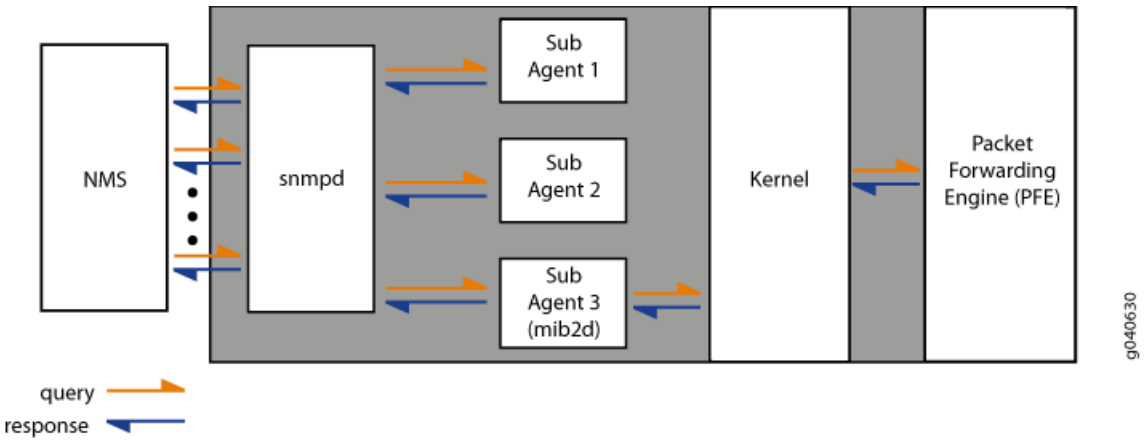
For more information about system logging severity levels for standard traps, see "Standard SNMP Traps Supported by Junos OS" on page 490. For more information about system logging severity levels for enterprise-specific traps, see "Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500.

SNMP Communication Flow

When a NMS polls the master agent for data, the master agent immediately shares the data with the NMS if the requested data is available from the master agent or one of the subagents. However, if the requested data does not belong to those categories that are maintained by the master agent or the subagents, the subagent polls the Junos OS kernel or the process that maintains that data. On receiving the required data, the subagent passes the response back to the master agent, which in turn passes it to the NMS.

Figure 25 on page 394 shows the communication flow among the NMS, SNMP master agent (snmpd), SNMP subagents, Junos OS kernel, and the Packet Forwarding Engine.

Figure 25: SNMP Communication Flow



When a significant event, most often an error or a failure, occurs on a network device, the SNMP agent sends notifications to the SNMP manager. The SNMP implementation in Junos OS supports two types of notifications: traps and informs. *Traps* are unconfirmed notifications, whereas *informs* are confirmed notifications. Informs are supported only on devices that support SNMP version 3 (SNMPv3) configuration.

Trap Queuing

Junos OS supports trap queuing to ensure that traps are not lost because of temporary unavailability of routes. Two types of queues, *destination queues* and a *throttle queue*, are formed to ensure delivery of traps and to control the trap traffic.

> **NOTE:** You cannot configure trap queueing in Junos OS. You cannot view information about trap queues except for what is provided in the system logs.

Junos OS forms a destination queue when a trap to a particular destination is returned because the host is not reachable, and adds the subsequent traps to the same destination to the queue. Junos OS checks for availability of routes every 30 seconds and sends the traps from the destination queue in a round-robin fashion.

If the trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts occur at progressive intervals of 1 minute, 2 minutes, 4 minutes, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is 10. After 10 unsuccessful attempts, the destination queue and all the traps in the queue are deleted.

Junos OS also has a throttle mechanism to control the number of traps (throttle threshold; default value of 500 traps) sent during a particular time period (throttle interval; default of 5 seconds) and to ensure consistency in trap traffic, especially when large number of traps are generated because of interface status changes. The throttle interval period begins when the first trap arrives at the throttle. All traps within the trap threshold are processed, and the traps beyond the threshold limit are queued.

The maximum size of trap queues—that is, throttle queue and destination queue put together—is 40,000. However, on EX Series Ethernet Switches, the maximum size of the trap queue is 1,000. The maximum size of any one queue is 20,000 for devices other than EX Series Switches. On EX Series Switches, the maximum size of one queue is 500. When a trap is added to the throttle queue, or if the throttle queue has exceeded the maximum size, the trap is added back on top of the destination queue, and all subsequent attempts from the destination queue are stopped for a 30-second period, after which the destination queue restarts sending the traps.

NOTE: Users cannot configure the Junos OS for trap queuing. Users cannot view any information about trap queues except what is available in the logged information.

RELATED DOCUMENTATION

- Best Practices for Configuring SNMP | **558**
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | **758**
- Optimizing the Network Management System Configuration for the Best Results | **555**
- Configuring Options on Managed Devices for Better SNMP Response Time | **556**
- Managing Traps and Informs | **432**
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | **643**

SNMPv3 Overview

In contrast to SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2), SNMP version 3 (SNMPv3) supports authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.

USM uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured for both the agent and the manager. Messages sent using USM are better protected than messages sent with community strings, where passwords are sent in the clear. With USM, messages exchanged between the manager and the agent can have data integrity checking and data origin authentication. USM protects against message delays and message replays by using time indicators and request IDs. Encryption is also available.

To complement the USM, SNMPv3 uses the VACM, a highly granular access-control model for SNMPv3 applications. Based on the concept of applying security policies to the name of the groups querying the agent, the agent decides whether the group is allowed to view or change specific MIB objects. VACM defines collections of data (called views), groups of data users, and access statements that define which views a particular group of users can use for reading, writing, or receiving traps.

Trap entries in SNMPv3 are created by configuring the notify, notify filter, target address, and target parameters. The **notify** statement specifies the type of notification (trap) and contains a single tag. The tag defines a set of target addresses to receive a trap. The notify filter defines access to a collection of trap object identifiers (OIDs). The target address defines a management application's address and other attributes to be used in sending notifications. Target parameters define the message processing and security parameters to be used in sending notifications to a particular management target.

To configure SNMPv3, perform the following tasks:

- Creating SNMPv3 Users on page 662
- Configuring MIB Views on page 612
- Defining Access Privileges for an SNMP Group on page 669
- Configuring SNMPv3 Traps on a Device Running Junos OS on page 678
- Configuring SNMP Informs on page 692

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

SNMPv3 Overview (QFX in Standalone Mode)

The QFX3500 switch supports SNMP version 3 (SNMPv3). SNMPv3 enhances the functionality of SNMPv1 and SNMPv2c by supporting user authentication and data encryption. SNMPv3 uses the user-based security model (USM) to provide security for SNMP messages, and the view-based access control model (VACM) for user access control.

SNMPv3 features include:

- With USM, the SNMP messages between the SNMP manager and the agent can have the message source authenticated and the data integrity checked. USM reduces messaging delays and message replays by enforcing timeout limits and by checking for duplicate message request IDs.
- VACM complements USM by providing user access control for SNMP queries to the agent. You define access privileges that you wish to extend to a group of one or more users. Access privileges are determined

by the security model parameters (**usm**, **v1**, or **v2**) and security level parameters (**authentication**, **privacy**, or **none**). For each security level, you must associate one MIB view for the group. Associating a MIB view with a group grants the read, write, or notify permission to a set of MIB objects for the group.

- You configure security parameters for each user, including the username, authentication type and authentication password, and privacy type and privacy password. The username given to each user is in a format that is dependent on the security model configured for that user.
- To ensure messaging security, another type of username, called the security name, is included in the messaging data that is sent between the local SNMP server and the destination SNMP server. Each user name is mapped to a security name, but the security name is in a format that is independent of the security model.
- Trap entries in SNMPv3 are created by configuring the notify, notify filter, target address, and target parameters. The **notify** statement specifies the type of notification (trap) and contains a single tag that defines a set of target addresses to receive a trap. The notify filter defines access to a collection of trap object identifiers (OIDs). The target address defines the address of an SNMP management application and other attributes used in sending notifications. Target parameters define the message processing and security parameters used in sending notifications to a particular target.

RELATED DOCUMENTATION

Assigning a Security Name to a Group

Configuring Access Privileges for a Group

Configuring SNMP Informs | **692**

Creating SNMPv3 Users | **662**

Loading MIB Files to a Network Management System

For your network management system (NMS) to identify and understand the MIB objects used by the Junos OS, you must first load the MIB files to your NMS using a MIB compiler. A MIB compiler is a utility that parses the MIB information such as the MIB object name, IDs, and data type for the NMS.

You can download the Junos MIB package from the Junos OS Enterprise MIBs index at https://www.juniper.net/documentation/en_US/release-independent/junos/mibs/mibs.html . The Junos MIB package is available in **.zip** and **.tar** packages. You can download the appropriate format based on your requirements.

The Junos MIB package contains two folders: **StandardMibs** and **JuniperMibs**. The **StandardMibs** folder contains the standard MIBs and RFCs that are supported on devices running the Junos OS, whereas the **JuniperMibs** folder contains the Juniper Networks enterprise-specific MIBs.

To load MIB files that are required for managing and monitoring devices running the Junos OS:

1. Go to the SNMP MIB Explorer Download page for Juniper Networks SNMP MIB packages (SNMP MIB Explorer).

2. Click the **TAR** or **ZIP** link under the appropriate release heading to download the Junos MIB package for that release.

3. Decompress the file (**.tar** or **.zip**) using an appropriate utility.

4. Load the standard MIB files (from the **StandardMibs** folder) in the following order:

   > **NOTE:** Some of the MIB compilers that are commonly used have the standard MIBs preloaded on them. If the standard MIBs are already loaded on the MIB compiler that you are using, skip this step and proceed to Step 7.

   a. **mib-SNMPv2-SMI.txt**
   b. **mib-SNMPv2-TC.txt**
   c. **mib-IANAifType-MIB.txt**
   d. **mib-IANA-RTPROTO-MIB.txt**
   e. **mib-rfc1907.txt**
   f. **mib-rfc4293.txt**
   g. **mib-rfc2012a.txt**
   h. **mib-rfc2013a.txt**
   i. **mib-rfc2863a.txt**

5. Load the remaining standard MIB files.

   > **NOTE:** You must follow the order specified in this procedure, and ensure that all standard MIBs are loaded before you load the enterprise-specific MIBs. There might be dependencies that require a particular MIB to be present on the compiler before loading some other MIB. You can find such dependencies listed in the **IMPORT** section of the MIB file.

6. Load the Juniper Networks enterprise-specific SMI MIB, **mib-jnx-smi.txt**, and the following optional SMI MIBs based on your requirements:

   - **mib-jnx-js-smi.txt**—(Optional) For Juniper Security MIB tree objects

- **mib-jnx-ex-smi.txt**—(Optional) For EX Series Ethernet Switches
- **mib-jnx-exp.txt**—(Recommended) For Juniper Networks experimental MIB objects

7. Load the remaining enterprise-specific MIBs from the **JuniperMibs** folder.

> **TIP:** While loading a MIB file, if the compiler returns an error message saying that any of the objects is undefined, open the MIB file using a text editor and ensure that all the MIB files listed in the **IMPORT** section are loaded on the compiler. If any of the MIB files listed in the **IMPORT** section is not loaded on the compiler, load that MIB file, and then try to load the MIB file that failed to load.
>
> For example, the enterprise-specific PING MIB, **mib-jnx-ping.txt**, has dependencies on RFC 2925, DiSMAN-PING-MIB, **mib-rfc2925a.txt**. If you try to load **mib-jnx-ping.txt** before loading **mib-rfc2925a.txt**, the compiler returns an error message saying that certain objects in **mib-jnx-ping.txt** are undefined. Load **mib-rfc2925a.txt**, and then try to load **mib-jnx-ping.txt**. The enterprise-specific PING MIB, **mib-jnx-ping.txt**, then loads without any issue.

RELATED DOCUMENTATION

Standard SNMP MIBs Supported by Junos OS | 452

Enterprise-Specific SNMP MIBs Supported by Junos OS | 436

show snmp

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.
- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the **show snmp health-monitor** command:

user@switch> show snmp health-monitor

```
Alarm
Index  Variable description                            Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                          58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                           0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                             0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                         35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                         0 active
       Chassis daemon                                     50 active
       Firewall daemon                                     0 active
       Interface daemon                                    5 active
       SNMP daemon                                        11 active
       MIB2 daemon                                        42 active
       ...
```

The following example provides sample output from the **show snmp mib** command:

user@switch> show snmp mib walk system

```
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the **show snmp statistics** command:

user@switch> show snmp statistics

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
    Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

RELATED DOCUMENTATION

- health-monitor | 2175
- show snmp mib | 2881
- show snmp statistics | 2904

Junos OS SNMP FAQ Overview

This document presents the most frequently asked questions about the features and technologies used to implement SNMP services on Juniper Networks devices using the Junos operating system.

SNMP enables users to monitor network devices from a central location. Many network management systems (NMS) are based on SNMP, and support for this protocol is a key feature of most network devices.

Juniper Networks provides many different platforms that support SNMP on the Junos OS. The Junos OS includes an onboard SNMP agent that provides remote management applications with access to detailed information about the devices on the network.

A typical SNMP implementation contains three components:

- Managed devices – Such as routers and switches.
- SNMP agent – Process that resides on a managed device and communicates with the NMS.
- NMS – Acombination of hardware and software used to monitor and administer the network; network device that runs SNMP manager software. Also referred to as an SNMP manager.

The SNMP agent exchanges network management information with the SNMP manager (NMS). The agent responds to requests for information and actions from the manager. The SNMP manager collects information about network connectivity, activity, and events by polling managed devices.

SNMP implementation in the Junos OS uses a master SNMP agent (known as an SNMP process or snmpd) that resides on the managed device. Various subagents reside on different modules of the Junos OS as well (such as the Routing Engine), and these subagents are managed by the snmpd.

RELATED DOCUMENTATION

Junos OS SNMP FAQs | **402**

Junos OS SNMP FAQs

IN THIS SECTION

- Junos OS SNMP Support FAQs | **403**
- Junos OS MIBs FAQs | **404**
- Junos OS SNMP Configuration FAQs | **412**
- SNMPv3 FAQs | **417**
- SNMP Interaction with Juniper Networks Devices FAQs | **419**
- SNMP Traps and Informs FAQs | **421**
- Junos OS Dual Routing Engine Configuration FAQs | **428**
- SNMP Support for Routing Instances FAQs | **429**
- SNMP Counters FAQs | **431**

This Frequently Asked Questions technology overview covers these SNMP-related areas:

Junos OS SNMP Support FAQs

This section presents frequently asked questions and answers related to SNMP support on Junos OS.

Which SNMP versions does Junos OS support?

Junos OS supports SNMP version 1 (SNMPv1), version 2 (SNMPv2c), and version 3 (SNMPv3). By default, SNMP is disabled on a Juniper Networks device.

Which ports (sockets) does SNMP use?

The default port for SNMP queries is port 161. The default port for SNMP traps and informs is port 162. The port used for SNMP traps and informs is configurable, and you can configure your system to use ports other than the default port 162. However, the SNMP listening port will remain the same; this is established on the RFC.

Is SNMP support different among the Junos OS platforms?

No, SNMP support is not different among the Junos OS platforms. SNMP configuration, interaction, and behavior are the same on any Junos OS device. The only difference that might occur across platforms is MIB support.

See also SNMP MIB Explorer for a list of MIBs that are supported across the Junos OS platforms.

Does Junos OS support the user-based security model (USM)?

Yes, Junos OS supports USM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined USM. SNMPv3 USM provides message security through data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload.

Does Junos OS support the view-based access control model (VACM)?

Yes, Junos OS supports VACM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined VACM. SNMPv3 VACM determines whether a specific type of access (read or write) to the management information is allowed.

Does Junos OS support SNMP informs?

Yes, Junos OS supports SNMP informs as part of its support for SNMPv3. SNMP informs are confirmed notifications sent from SNMP agents to SNMP managers when significant events occur on a network device. When an SNMP manager receives an inform, it sends a response to the sender to verify receipt of the inform.

Can I provision or configure a device using SNMP on Junos OS?

No, provisioning or configuring a device using SNMP is not allowed on Junos OS.

RELATED DOCUMENTATION

Junos OS MIBs FAQs

This section presents frequently asked questions and answers related to Junos OS MIBs.

What is a MIB?

A management information base (MIB) is a table of definitions for managed objects in a network device. MIBs are used by SNMP to maintain standard definitions of all of the components and their operating conditions within a network device. Each object in the MIB has an identifying code called an object identifier (OID).

MIBs are either standard or enterprise-specific. Standard MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer.

For a list of supported standard MIBs, see "Standard SNMP MIBs Supported by Junos OS" on page 452.

For a list of Juniper Networks enterprise-specific MIBs, see "Enterprise-Specific SNMP MIBs Supported by Junos OS" on page 436.

Do MIB files reside on the Junos OS devices?

No, MIB files do not reside on the Junos OS devices. You must download the MIB files from the Juniper Networks Technical Publications page for the required Junos OS release: https://www.juniper.net/documentation/en_US/release-independent/junos/mibs/mibs.html .

How do I compile and load the Junos OS MIBs onto an SNMP manager or NMS?

For your network management systems (NMSs) to identify and understand the MIB objects used by Junos OS, you must first load the MIB files to your NMS using a MIB compiler. A MIB compiler is a utility that parses the MIB information, such as the MIB object names, IDs, and data types for the NMS.

You can download the Junos OS MIB package from the Enterprise-Specific MIBs and Traps section at https://www.juniper.net/documentation/en_US/release-independent/junos/mibs/mibs.html or https://www.juniper.net/documentation/software/junos/index.html .

The Junos OS MIB package has two folders: **StandardMibs**, containing standard MIBs supported on Juniper Networks devices, and **JuniperMibs**, containing Juniper Networks enterprise-specific MIBs. You *must* have the required standard MIBs downloaded and decompressed before downloading any enterprise-specific MIBs. There might be dependencies that require a particular standard MIB to be present on the compiler before loading a particular enterprise-specific MIB.

The Junos OS MIB package is available in **.zip** and **.tar** formats. Download the format appropriate for your requirements.

Use the following steps to load MIB files for devices running Junos OS:

1. Navigate to the appropriate Juniper Networks software download page and locate the **Enterprise MIBs** link under the **Enterprise-Specific MIBs and Traps** section.

   > **NOTE:** Although the link is titled **Enterprise MIBs**, both standard MIBs and enterprise-specific MIBs are available for download from this location.

2. Click the **TAR** or **ZIP** link to download the Junos OS MIB package.

3. Decompress the file (**.tar** or **.zip**) using an appropriate utility.

   > **NOTE:** Some commonly used MIB compilers are preloaded with standard MIBs. You can skip Step 4 and Step 5 and proceed to Step 6 if you already have the standard MIBs loaded on your system.

4. Load the standard MIB files from the **StandardMibs** folder.

   Load the files in the following order:

   a. mib-SNMPv2-SMI.txt
   b. mib-SNMPv2-TC.txt
   c. mib-IANAifType-MIB.txt
   d. mib-IANA-RTPROTO-MIB.txt
   e. mib-rfc1907.txt
   f. mib-rfc2011a.txt
   g. mib-rfc2012a.txt
   h. mib-rfc2013a.txt
   i. mib-rfc2863a.txt

5. Load any remaining standard MIB files.

> **NOTE:** You must follow the order specified in this procedure, and ensure that all standard MIBs are loaded before you load the enterprise-specific MIBs. There might be dependencies that require a particular standard MIB to be present on the compiler before loading a particular enterprise-specific MIB. Dependencies are listed in the **IMPORT** section of the MIB file.

6. After loading the standard MIBs, load the Juniper Networks enterprise-specific SMI MIB, **mib-jnx-smi.txt**, and the following optional SMI MIBs based on your requirements:
   - mib-jnx-exp.txt—(Recommended) for Juniper Networks experimental MIB objects
   - mib-jnx-js-smi.txt—(Optional) for Juniper Security MIB tree objects
   - mib-jnx-ex-smi.txt—(Optional) for EX Series Ethernet Switches
7. Load any remaining desired enterprise-specific MIBs from the **JuniperMibs** folder.

> **TIP:** While loading a MIB file, if the compiler returns an error message indicating that any of the objects are undefined, open the MIB file using a text editor and ensure that all the MIB files listed in the **IMPORT** section are loaded on the compiler. If any of the MIB files listed in the **IMPORT** section are not loaded on the compiler, load the missing file or files first, then try to load the MIB file that failed.
>
> The system might return an error if files are not loaded in a particular order.

What is SMI?

Structure of Management Information Version (SMI) is a subset of Abstract Syntax Notation One (ASN.1), which describes the structure of objects. SMI is the notation syntax, or “grammar”, that is the standard for writing MIBs.

Which versions of SMI does Junos OS support?

The Junos OS supports SMIv1 for SNMPv1 MIBs, and SMIv2 for SNMPv2c and enterprise MIBs.

Does Junos OS support MIB II?

Yes, Junos OS supports MIB II, the second version of the MIB standard.

The features of MIB II include:

- Additions that reflect new operational requirements.
- Backward compatibility with the original MIBs and SNMP.

- Improved support for multiprotocol entities.
- Improved readability.

Refer to the relevant release documentation for a list of MIBs that are supported. Go to https://www.juniper.net/documentation/software/junos/index.html .

Are the same MIBs supported across all Juniper Networks devices?

There are some common MIBs supported by all the Junos OS devices, such as the Interface MIB (ifTable), System MIB, and Chassis MIB. Some MIBs are supported only by functionalities on specific platforms. For example, the Bridge MIB is supported on the EX Series Ethernet Switches and the SRX Series Services Gateways for the branch.

What is the system object identifier (SYSOID) of a device? How do I determine the SYSOID of my device?

The jnx-chas-defines (Chassis Definitions for Router Model) MIB has a **jnxProductName** branch for every Junos OS device. The system object ID of a device is identical to the object ID of the **jnxProductName** for the platform. For example, for an M7i Multiservice Edge Router, the jnxProductNameM7i is .1.3.6.1.4.1.2636.1.1.1.2.10 in the jnxProductName branch, which is identical to the SYSOID of the M7i (.1.3.6.1.4.1.2636.1.1.1.2.10).

How can I determine if a MIB is supported on a platform? How can I determine which MIBs are supported by a device?

MIBs device and platform support is listed on the Junos OS Technical Documentation. See "Enterprise-Specific SNMP MIBs Supported by Junos OS" on page 436 and "Standard SNMP MIBs Supported by Junos OS" on page 452 documents to view the list of MIBs and supported Junos OS devices.

What can I do if the MIB OID query is not responding?

There can be various reasons why the MIB OID query stops responding. One reason could be that the MIB itself is unresponsive. To verify that the MIB responds, use the **show snmp mib walk | get *MIB name* | *MIB OID*** command:

- If the MIB responds, the communication issue exists between the SNMP master and SNMP agent. Possible reasons for this issue include network issues, an incorrect community configuration, an incorrect SNMP configuration, and so on.
- If the MIB does not respond, enable SNMP **traceoptions** to log PDUs and errors. All incoming and outgoing SNMP PDUs are logged. Check the **traceoptions** output to see if there are any errors.

If you continue to have problems with the MIB OID query, technical product support is available through the Juniper Networks Technical Assistance Center (JTAC).

What is the enterprise branch number for Junos OS?

The enterprise branch number for Junos OS is 2636. Enterprise branch numbers are used in SNMP MIB configurations, and they are also known as SMI network management private enterprise codes.

Which MIB displays the hardware and chassis details on a Juniper Networks device?

The Chassis MIB (jnxchassis.mib) displays the hardware and chassis details for each Juniper Networks device. It provides information about the router and its components. The Chassis MIB objects represent each component and its status.

Which MIB objects can I query to determine the CPU and memory utilization of the Routing Engine, Flexible PIC Concentrator (FPC), and PIC components on a device?

Query the Chassis MIB objects **jnxOperatingMemory**, **jnxOperatingtBuffer**, and **jnxOperatingCPU** to find out the CPU and memory utilization of the hardware components of a device.

Is the interface index (ifIndex) persistent?

The ifIndex is persistent when reboots occur if the Junos OS version remains the same, meaning the values assigned to the interfaces in the ifIndex do not change.

When there is a software upgrade, the device tries to keep the ifIndex persistent on a best effort basis. For Junos OS Release 10.0 and earlier, the ifIndex is not persistent when there is a software upgrade to Junos OS Release 10.1 and later.

Is it possible to set the ifAdminStatus?

SNMP is not allowed to set the ifAdminStatus.

Which MIB objects support SNMP set operations?

The Junos OS SNMP set operations are supported in the following MIB tables and variables:

- snmpCommunityTable
- eventTable
- alarmTable
- snmpTargetAddrExtTable
- jnxPingCtlTable
- pingCtlTable
- traceRouteCtlTable
- jnxTraceRouteCtlTable
- sysContact.0
- sysName.0
- sysLocation.0
- pingMaxConcurrentRequests.0
- traceRouteMaxConcurrentRequests.0

- usmUserSpinLock
- usmUserOwnAuthKeyChange
- usmUserPublic
- vacmSecurityToGroupTable (vacmGroupName, vacmSecurityToGroupStorageType, and vacmSecurityToGroupStatus)
- vacmAccessTable (vacmAccessContextMatch, vacmAccessReadViewName, vacmAccessWriteViewName, vacmAccessNotifyViewName, vacmAccessStorageType, and vacmAccessStatus)
- vacmViewSpinLock
- vacmViewTreeFamilyTable (vacmViewTreeFamilyMask, vacmViewTreeFamilyType, vacmViewTreeFamilyStorageType, and vacmViewTreeFamilyStatus)

Does Junos OS support remote monitoring (RMON)?

Yes, Junos OS supports RMON as defined in RFC 2819, *Remote Network Monitoring Management Information Base*. However, remote monitoring version 2 (RMON 2) is not supported.

Can I use SNMP to determine the health of the processes running on the Routing Engine?

Yes, you can use SNMP to determine the health of the Routing Engine processes by configuring the health monitoring feature. On Juniper Networks devices, RMON alarms and events provide much of the infrastructure needed to reduce the polling overhead from the NMS. However, you must set up the NMS to configure specific MIB objects into RMON alarms. This often requires device-specific expertise and customizing the monitoring application. Additionally, some MIB object instances that need monitoring are set only at initialization, or they change at runtime and cannot be configured in advance.

To address these issues, the health monitor extends the RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances, such as file system usage, CPU usage, and memory usage, and includes support for unknown or dynamic object instances, such as Junos OS software processes.

To display the health monitoring configuration, use the **show snmp health-monitor** command:

```
user@host> show snmp health-monitor
interval 300;
rising-threshold 90;
falling-threshold 80;
```

When you configure the health monitor, monitoring information for certain object instances is available, as shown in Table 28 on page 410.

Table 28: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed.1	Monitors the following file system on the router or switch: /dev/ad0s1a: This is the root file system mounted on **/**.
jnxHrStoragePercentUsed.2	Monitors the following file system on the router or switch: /dev/ad0s1e: This is the configuration file system mounted on **/config**.
jnxOperatingCPU (RE0)	Monitor CPU usage for Routing Engines RE0 and RE1. The index values assigned to the Routing Engines depend on whether the Chassis MIB uses a zero-based or a ones-based indexing scheme. Because the indexing scheme is configurable, the correct index is determined whenever the router is initialized and when there is a configuration change. If the router or switch has only one Routing Engine, the alarm entry monitoring RE1 is removed after five failed attempts to obtain the CPU value.
jnxOperatingCPU (RE1)	
jnxOperatingBuffer (RE0)	Monitor the amount of memory available on Routing Engines RE0 and RE1. Because the indexing of this object is identical to that used for jnxOperatingCPU, index values are adjusted depending on the indexing scheme used in the Chassis MIB. As with jnxOperatingCPU, the alarm entry monitoring RE1 is removed if the router or switch has only one Routing Engine.
jnxOperatingBuffer (RE1)	
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS software process. Multiple instances of the same process are monitored and indexed separately.
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS software process. Multiple instances of the same process are monitored and indexed separately.

The system log entries generated for any health monitor events, such as thresholds crossed and errors, have a corresponding **HEALTHMONITOR** tag rather than a generic **SNMPD_RMON_EVENTLOG** tag. However, the health monitor sends generic RMON **risingThreshold** and **fallingThreshold** traps.

Are the Ping MIBs returned in decimal notation and ASCII?

Yes, both decimal notation and ASCII are supported, which is the standard implementation in SNMP. All strings are ASCII encoded.

The following example displays the Ping MIB in hexadecimal notation:

```
pingCtlTargetAddress.2.69.72.9.116.99.112.115.97.109.112.108.101 = 0a fa 01 02
```

This translates to ASCII:

```
pingCtlTargetAddress."EH"."tcpsample" = 0a fa 01 02
2= length of the string
69=E
72=H
9=length of second string
116=t
99 =c
112=p
115=s
97=a
109=m
112 =p
108 =l
101 =e
```

As of Junos OS Release 9.6 and later, the Junos OS CLI returns ASCII values using the command **show snmp mib *get* | *get-next* | *walk* ascii**.

The following example shows the output with the ASCII option:

`user@host>` **show snmp mib walk pingCtlTargetAddress ascii**

```
pingCtlTargetAddress."EH"."httpgetsample" = http://www.yahoo.com
pingCtlTargetAddress."p1"."t2" = 74 c5 b3 06
pingCtlTargetAddress."p1"."t3" = 74 c5 b2 0c
```

The following example shows the output without the ASCII option:

`user@host>` **show snmp mib walk pingCtlTargetAddress**

```
pingCtlTargetAddress.2.69.72.13.104.116.116.112.103.101.116.115.97.109.112.108.101
 = http://www.yahoo.com
pingCtlTargetAddress.2.112.49.2.116.50 = 74 c5 b3 06
pingCtlTargetAddress.2.112.49.2.116.51 = 74 c5 b2 0c
```

You can convert decimal and ASCII values using a decimal ASCII chart like the one at http://www.asciichart.com .

Is IPv6 supported by the Ping MIB for remote operations?

No, IPv6 is not supported.

Is there an SNMP MIB to show Address Resolution Protocol (ARP) table information? Are both IP and MAC addresses displayed in the same table?

Yes, the Junos OS supports the standard MIB **ipNetToMediaTable**, which is described in RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*. This table is used for mapping IP addresses to their corresponding MAC addresses.

RELATED DOCUMENTATION

Junos OS SNMP Configuration FAQs

This section presents frequently asked questions and answers related to Junos OS SNMP configuration.

Can the Junos OS be configured for SNMPv1 and SNMPv3 simultaneously?

Yes, SNMP has backward compatibility, meaning that all three versions can be enabled simultaneously.

Can I filter specific SNMP queries on a device?

Yes, you can filter specific SNMP queries on a device using **exclude** and **include** statements.

The following example shows a configuration that blocks read-write operation on all OIDs under .1.3.6.1.2.1.1 for the community **test**:

```
user@host# show snmp
view system-exclude {
   oid .1.3.6.1.2.1.1 exclude;
   oid .1 include;
}
   community test {
      view system-exclude;
      authorization read-write;
   }
```

Can I change the SNMP agent engine ID?

Yes, the SNMP agent engine ID can be changed to the MAC address of the device, the IP address of the device, or any other desired value. Several examples are included here.

The following example shows how to use the MAC address of a device as the SNMP agent engine ID:

```
user@host# show snmp
engine-id {
    use-mac-address;
}
```

The following example shows how to use the IP address of a device as the SNMP agent engine ID:

```
user@host# show snmp
engine-id {
    use-default-ip-address;
}
```

The following example shows the use of a selected value, **AA** in this case, as the SNMP agent engine ID of a device:

```
user@host# show snmp
engine-id {
    local AA;
}
```

How can I configure a device with dual Routing Engines or a chassis cluster (SRX Series Services Gateways) for continued communication during a switchover?

When configuring for continued communication, the SNMP configuration should be identical between the Routing Engines. However, it is best to have separate Routing Engine IDs configured for each Routing Engine, especially when using SNMPv3.

The following example shows the configuration of the Routing Engines in a dual Routing Engine device. Notice that the Routing Engine IDs are set to the MAC addresses for each Routing Engine:

```
user@host# show groups
re0 {
    system {
        host-name PE3-re0;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 116.197.178.14/27;
                    address 116.197.178.29/27 {
```

```
                master-only;
            }
        }
    }
  }
  snmp {
    engine-id {
      use-mac-address;
    }
  }
}
re1 {
  system {
    host-name PE3-re1;
  }
  interfaces {
    fxp0 {
      unit 0 {
        family inet {
          address 116.197.178.11/27;
          address 116.197.178.29/27 {
            master-only;
          }
        }
      }
    }
  }
  snmp {
    engine-id {
      use-mac-address;
    }
  }
}
```

The following is an example of an SNMPv3 configuration on a dual Routing Engine device:

```
user@host> show snmp name host1
v3 {
  vacm {
    security-to-group {
      security-model usm {
        security-name test123 {
          group test1;
```

```
            }
            security-name juniper {
                group test1;
            }
        }
    }
    access {
        group test1 {
            default-context-prefix {
                security-model any {
                    security-level authentication {
                        read-view all;
                    }
                }
            }
            context-prefix MGMT_10 {
                security-model any {
                    security-level authentication {
                        read-view all;
                    }
                }
            }
        }
    }
}
target-address server1 {
    address 116.197.178.20;
    tag-list router1;
    routing-instance MGMT_10;
    target-parameters test;
}
target-parameters test {
    parameters {
        message-processing-model v3;
        security-model usm;
        security-level authentication;
        security-name juniper;
    }
    notify-filter filter1;
}
notify server {
    type trap;
    tag router1;
}
```

```
    notify-filter filter1 {
        oid .1 include;
    }
    view all {
        oid .1 include;
    }
    community public {
        view all;
    }
    community comm1;
    community comm2;
    community comm3 {
        view all;
        authorization read-only;
        logical-system LDP-VPLS {
            routing-instance vpls-server1;
        }
    }
    trap-group server1 {
        targets {
            116.197.179.22;
        }
    }
    routing-instance-access;
    traceoptions {
        flag all;
    }
}
```

How can I track SNMP activities?

SNMP trace operations track activity of SNMP agents and record the information in log files.

A sample **traceoptions** configuration might look like this:

```
[edit snmp]
user@host# set traceoptions flag all
```

When the **traceoptions flag all** statement is included at the **[edit snmp]** hierarchy level, the following log files are created:

- snmpd
- mib2d
- rmopd

RELATED DOCUMENTATION

Junos OS SNMP Support FAQs | 403
Junos OS MIBs FAQs | 404
SNMPv3 FAQs | 417
SNMP Interaction with Juniper Networks Devices FAQs | 419
SNMP Traps and Informs FAQs | 421
SNMP Support for Routing Instances FAQs | 429
SNMP Counters FAQs | 431

SNMPv3 FAQs

This section presents frequently asked questions and answers related to SNMPv3.

Why is SNMPv3 important?

SNMP v3 provides enhanced security compared to the other versions of SNMP. It provides authentication and encryption of data. Enhanced security is important for managing devices at remote sites from the management stations.

In my system, the MIB object snmpEngineBoots is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Yes, this is the expected behavior. Each Routing Engine runs its own SNMP process (snmpd), allowing each Routing Engine to maintain its own engine boots. However, if both routing engines have the same engine ID and the routing engine with lesser **snmpEngineBoots** value is selected as the master routing engine during the switchover process, the **snmpEngineBoots** value of the master routing engine is synchronized with the **snmpEngineBoots** value of the other routing engine.

Do I need the SNMP manager engine object identifier (OID) for informs?

Yes, the engine OID of the SNMP manager is required for authentication, and informs do not work without it.

I see the configuration of informs under the [edit snmp v3] hierarchy. Does this mean I cannot use informs with SNMPv2c?

Informs can be used with SNMPv2c. The following example shows the basic configuration for SNMPv3 informs on a device (note that the authentication and privacy is set to none):

```
[edit snmp]
v3 {
   usm {
      remote-engine 00000063000100a2c0a845b3 {
```

```
        user RU2_v3_sha_none {
            authentication-none;
            privacy-none;
        }
    }
}
vacm {
    security-to-group {
        security-model usm {
            security-name RU2_v3_sha_none {
                group g1_usm_auth;
            }
        }
    }
    access {
        group g1_usm_auth {
            default-context-prefix {
                security-model usm {
                    security-level authentication {
                        read-view all;
                        write-view all;
                        notify-view all;
                    }
                }
            }
        }
    }
}
target-address TA2_v3_sha_none {
    address 192.168.69.179;
    tag-list tl1;
    address-mask 255.255.252.0;
    target-parameters TP2_v3_sha_none;
}
target-parameters TP2_v3_sha_none {
    parameters {
        message-processing-model v3;
        security-model usm;
        security-level none;
        security-name RU2_v3_sha_none;
    }
    notify-filter nf1;
}
notify N1_all_tl1_informs {
```

```
        type inform; # Replace “inform” with “trap” to convert informs to traps.
        tag tl1;
    }
    notify-filter nf1 {
        oid .1 include;
    }
    view all {
        oid .1 include;
    }
}
```

You can convert the SNMPv3 informs to traps by setting the value of the **type** statement at the **[edit snmp v3 notify N1_all_tl1_informs]** hierarchy level to **trap** as shown in the following example:

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

RELATED DOCUMENTATION

SNMP Interaction with Juniper Networks Devices FAQs

This section presents frequently asked questions and answers related to how SNMP interacts with Juniper Networks devices.

How frequently should a device be polled? What is a good polling rate?

It is difficult to give an absolute number for the rate of SNMP polls per second since the rate depends on the following two factors:

- The number of variable bindings in a protocol data unit (PDU)
- The response time for an interface from the Packet Forwarding Engine

In a normal scenario where no delay is being introduced by the Packet Forwarding Engine and there is one variable per PDU (a Get request), the response time is 130+ responses per second. However, with multiple variables in an SNMP request PDU (30 to 40 for GetBulk requests), the number of responses per second is much less. Because the Packet Forwarding Engine load can vary for each system, there is greater variation in how frequently a device should be polled.

Frequent polling of a large number of counters, especially statistics, can impact the device. We recommend the following optimization on the SNMP managers:

- Use the row-by-row polling method, not the column-by-column method.
- Reduce the number of variable bindings per PDU.

- Increase timeout values in polling and discovery intervals.
- Reduce the incoming packet rate at the SNMP process (snmpd).

For better SNMP response on the device, the Junos OS does the following:

- Filters out duplicate SNMP requests.
- Excludes interfaces that are slow in response from SNMP queries.

One way to determine a rate limit is to note an increase in the **Currently Active** count from the **show snmp statistics extensive** command.

The following is a sample output of the **show snmp statistics extensive** command:

`user@host>` **show snmp statistics extensive**

```
SNMP statistics:
 Input:
   Packets: 226656, Bad versions: 0, Bad community names: 0,
   Bad community uses: 0, ASN parse errors: 0,
   Too bigs: 0, No such names: 0, Bad values: 0,
   Read onlys: 0, General errors: 0,
   Total request varbinds: 1967606, Total set varbinds: 0,
   Get requests: 18478, Get nexts: 75794, Set requests: 0,
   Get responses: 0, Traps: 0,
   Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
   Throttle drops: 27084, Duplicate request drops: 0
 V3 Input:
   Unknown security models: 0, Invalid messages: 0
   Unknown pdu handlers: 0, Unavailable contexts: 0
   Unknown contexts: 0, Unsupported security levels: 0
   Not in time windows: 0, Unknown user names: 0
   Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
 Output:
   Packets: 226537, Too bigs: 0, No such names: 0,
   Bad values: 0, General errors: 0,
   Get requests: 0, Get nexts: 0, Set requests: 0,
   Get responses: 226155, Traps: 382
 SA Control Blocks:
   Total: 222984, Currently Active: 501, Max Active: 501,
   Not found: 0, Timed Out: 0, Max Latency: 25
 SA Registration:
   Registers: 0, Deregisters: 0, Removes: 0
 Trap Queue Stats:
   Current queued: 0, Total queued: 0, Discards: 0, Overflows: 0
 Trap Throttle Stats:
```

```
    Current throttled: 0, Throttles needed: 0
  Snmp Set Stats:
    Commit pending failures: 0, Config lock failures: 0
    Rpc failures: 0, Journal write failures: 0
    Mgd connect failures: 0, General commit failures: 0
```

Does SNMP open dynamic UDP ports? Why?

The SNMP process opens two additional ports (sockets): one for IPv4 and one for IPv6. This enables the SNMP process to send traps.

I am unable to perform a MIB walk on the ifIndex. Why is this?

Any variable bindings or values with an access level of **not-accessible** cannot be queried directly because they are part of other variable bindings in the SNMP MIB table. The ifIndex has an access level of **not-accessible**. Therefore, it cannot be accessed directly because it is part of the variable bindings. However, the ifIndex can be accessed indirectly through the variable bindings.

I see SNMP_IPC_READ_ERROR messages when the SNMP process restarts on my system and also during Routing Engine switchover. Is this acceptable?

Yes, it is acceptable to see **SNMP_IPC_READ_ERROR** messages when the SNMP process is restarted, the system reboots, or during a Routing Engine switchover. If all the processes come up successfully and the SNMP operations are working properly, then these messages can be ignored.

What is the source IP address used in the response PDUs for SNMP requests? Can this be configured?

The source IP address used in the response PDUs for SNMP requests is the IP address of the outgoing interface to reach the destination. The source IP address cannot be configured for responses. It can only be configured for traps.

RELATED DOCUMENTATION

SNMP Traps and Informs FAQs

This section presents frequently asked questions and answers related to SNMP traps and informs.

Does the Junos OS impose any rate limiting on SNMP trap generation?

The Junos OS implements a trap-queuing mechanism to limit the number of traps that are generated and sent.

If a trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts occur at progressive intervals of 1,

2, 4, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is 10. After 10 unsuccessful attempts, the destination queue and all traps in the queue are deleted.

Junos OS also has a throttle threshold mechanism to control the number of traps sent (default 500 traps) during a particular throttle interval (default 5 seconds). This helps ensure consistency in trap traffic, especially when a large number of traps are generated due to interface status changes.

The throttle interval begins when the first trap arrives at the throttle. All traps within the throttle threshold value are processed, and traps exceeding the threshold value are queued. The maximum size of all trap queues (the throttle queue and the destination queue) is 40,000 traps. The maximum size of any one queue is 20,000 traps. When a trap is added to the throttle queue, or if the throttle queue has exceeded the maximum size, the trap is moved to the top of the destination queue. Further attempts to send the trap from the destination queue are stopped for a 30-second period, after which the destination queue restarts sending the traps.

> **NOTE:** For the Juniper Networks EX Series Ethernet Switch, the maximum size of all trap queues (the throttle queue and the destination queue) is 1,000 traps. The maximum size for any one queue on the EX Series is 500 traps.

I did not see a trap when I had a syslog entry with a critical severity. Is this normal? Can it be changed?

Not every syslog entry with critical severity is a trap. However, you can convert any syslog entry to a trap using the **event-options** statement.

The following example shows how to configure a **jnxSyslogTrap** whenever an **rpd_ldp_nbrdown** syslog entry message error occurs.

```
user@host> show event-options
policy snmptrap {
   events rpd_ldp_nbrdown;
   then {
      raise-trap;
   }
}
```

Are SNMP traps compliant with the Alarm Reporting Function (X.733) on the Junos OS?

No, SNMP traps on the Junos OS are not X.733 compliant.

Can I set up filters for traps or informs?

Traps and informs can be filtered based on the trap category and the object identifier. You can specify categories of traps to receive per host by using the **categories** statement at the **[edit snmp trap-group**

trap-group] hierarchy level. Use this option when you want to monitor only specific modules of the Junos OS.

The following example shows a sample configuration for receiving only **link**, **vrrp-events**, **services**, and **otn-alarms** traps:

```
[edit snmp]
trap-group jnpr {
    categories {
        link;
        vrrp-events;
        services;
        otn-alarms;
    }
    targets {
        192.168.69.179;
    }
}
```

The Junos OS also has a more advanced filter option (**notify-filter**) for filtering specific traps or a group of traps based on their object identifiers.

The SNMPv3 configuration also supports filtering of SNMPv1 and SNMPv2 traps and excluding Juniper Networks enterprise-specific configuration management traps, as shown in the following configuration example:

```
[edit snmp]
v3 {
    vacm {
        security-to-group {
            security-model v2c {
                security-name sn_v2c_trap {
                    group gr_v2c_trap;
                }
            }
        }
        access {
            group gr_v2c_trap {
                default-context-prefix {
                    security-model v2c {
                        security-level none {
                            read-view all;
                            notify-view all;
                        }
```

```
                }
            }
        }
    }
    target-address TA_v2c_trap {
        address 10.209.196.166;
        port 9001;
        tag-list tg1;
        target-parameters TP_v2c_trap;
    }
    target-parameters TP_v2c_trap {
        parameters {
            message-processing-model v2c;
            security-model v2c;
            security-level none;
            security-name sn_v2c_trap;
        }
        notify-filter nf1;
    }
    notify v2c_notify {
        type trap;
        tag tg1;
    }
    notify-filter nf1 {
        oid .1.3.6.1.4.1.2636.4.5 exclude;
        oid .1 include;
    }
    snmp-community index1 {
        community-name "$9$tDLl01h7Nbw2axN"; ## SECRET-DATA
        security-name sn_v2c_trap;
        tag tg1;
    }
view all {
    oid .1 include;
}
}
```

Can I simulate traps on a device?

Yes, you can use the **request snmp spoof-trap *trap name*** command for simulating a trap to the NMS that normally receives your device's traps. You can also add required values using the **variable-bindings** parameter.

The following example shows how to simulate a trap to the local NMS using variable bindings:

```
user@host> request snmp spoof-trap linkDown variable-bindings "ifIndex[116]=116, ifAdminStatus[116]=1
  ,ifOperStatus[116]=2 , ifName[116]=ge-1/0/1"
```

How do I generate a warm start SNMPv1 trap?

When the SNMP process is restarted under normal conditions, a warm start trap is generated if the system up time is more than 5 minutes. If the system up time is less than 5 minutes, a cold start trap is generated.

The NMS sees only the MIB OIDs and numbers, but not the names of the SNMP traps. Why?

Before the NMS can recognize the SNMP trap details, such as the names of the traps, it must first compile and understand the MIBs and then parse the MIB OIDs.

In the Junos OS, how can I determine to which category a trap belongs?

For a list of common traps and their categories, see "Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500.

Can I configure a trap to include the source IP address?

Yes, you can configure the **source-address**, **routing-instance**, or **logical-instance** name for the source IP address using the **trap-options** command:

```
user@host> show snmp trap-options
source-address 10.1.1.1;
```

Can I create a custom trap?

Yes, you can use the **jnxEventTrap** event script to create customized traps as needed.

In the following example, a Junos OS operations (op) script is triggered when a **UI_COMMIT_NOT_CONFIRMED** event is received. The Junos OS op script matches the complete message of the event and generates an SNMP trap.

Example: Junos OS Op Script

```
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";

param $event;
param $message;
```

```
match / {

    /*
     * trapm utilty wants the following characters in the value to be escaped
     * '[', ']', ' ', '=', and ','
     */
    var $event-escaped = {
        call escape-string($text = $event, $vec = '[] =,');
    }

    var $message-escaped = {
        call escape-string($text = $message, $vec = '[] =,');
    }

    <op-script-results> {
 var $rpc = <request-snmp-spoof-trap> {
     <trap> "jnxEventTrap";
     <variable-bindings> "jnxEventTrapDescr[0]='Event-Trap' , "
  _ "jnxEventAvAttribute[1]='event' , "
  _ "jnxEventAvValue[1]='" _ $event-escaped _ "' , "
  _ "jnxEventAvAttribute[2]='message' , "
  _ "jnxEventAvValue[1]='" _ $message-escaped _ "'";
 }

 var $res = jcs:invoke($rpc);
    }
}

template escape-string ($text, $vec) {

    if (jcs:empty($vec)) {
        expr $text;

    } else {
        var $index = 1;
        var $from = substring($vec, $index, 1);
        var $changed-value = {
            call replace-string($text, $from) {
                with $to = {
                    expr "\\";
                    expr $from;
                 }
            }
```

```
        }

        call escape-string($text = $changed-value, $vec = substring($vec, $index
 + 1));
    }
}

template replace-string ($text, $from, $to) {

    if (contains($text, $from)) {
        var $before = substring-before($text, $from);
        var $after = substring-after($text, $from);
        var $prefix = $before _  $to;

        expr $before;
        expr $to;
        call replace-string($text = $after, $from, $to);

    } else {
        expr $text;
    }
}
```

After creating your customized trap, you must configure a policy on your device to tell the device what actions to take after it receives the trap.

Here is an example of a configured policy under the **[edit event-options]** hierarchy:

```
[edit event-options]
user@host> show
policy trap-on-event {
   events UI_COMMIT_NOT_CONFIRMED;
   attributes-match {
      UI_COMMIT_NOT_CONFIRMED.message matches complete;
   }
   then {
      event-script ev-syslog-trap.junos-op {
         arguments {
            event UI_COMMIT_NOT_CONFIRMED;
            message "{$$.message}";
         }
      }
```

```
    }
}
```

Can I disable link up and link down traps on interfaces?

Yes, link up and link down traps can be disabled in the interface configuration. To disable the traps, use the **no-traps** 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*]** hierarchies for physical and logical interfaces.

```
(traps | no-traps);
```

I see the link up traps on logical interfaces, but I do not see the link down traps. Is this normal behavior?

For Ethernet and ATM types of interfaces, Junos OS does not send link down traps for a logical interface if the physical interface is down to prevent flooding alarms for the same root cause. However, when the physical interface and logical interfaces come back up, traps are sent indicating link up. This is because the physical interface coming up does not necessarily mean the logical interfaces are also coming up.

For SONET types of interfaces with PPP encapsulation, Junos OS does send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For SONET types of interfaces with HDLC encapsulation, Junos OS does not send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For channelize interfaces with PPP encapsulation, Junos OS does send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For channelize interfaces with HDLC encapsulation, Junos OS does not send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

RELATED DOCUMENTATION

Junos OS Dual Routing Engine Configuration FAQs

This section presents frequently asked questions and answers related to the configuration of dual Routing Engines.

The SNMP configuration should be identical between the Routing Engines when configuring for continued communication. However, we recommend having separate Routing Engine IDs configured for each Routing Engine, when using SNMPv3.

In my system, the MIB object snmpEngineBoots is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Yes. This is the normal behavior. Each Routing Engine runs its own SNMP process (snmpd) agent, allowing each Routing Engine to maintain its own engine boots.

Is there a way to identify that an address belongs to RE0, RE1, or the master Routing Engine management interface (fxp0) by looking at an SNMP walk?

No. When you do an SNMP walk on the device, it only displays the master Routing Engine management interface address.

What is the best way to tell if the current IP address belongs to fxp0 or a Routing Engine, from a CLI session?

Routing Engines are mapped with the **fxp0** interface. This means that when you query RE0, the ifTable reports the **fxp0** interface address of RE0 only. Similarly, if you query RE1, the ifTable reports the **fxp0** interface address of RE1 only.

When there is a failover, the master hostname is changed since the hostname belongs to the Routing Engine. Is this correct?

Yes. You can configure the same hostname or different hostnames. Either would work.

If only the master IP address is configured (for example, 192.168.2.5), and the **sysDescr.0** object has the same string configured on both of the Routing Engines, then even after a switchover, the **sysDescr.0** object returns the same value. The following sample shows the results you get by using the **snmpget** command:

```
bng-junos-pool02: /c/svivek/PR_BRANCH/src> snmpget -c jnpr -v2c 192.168.2.5
sysDescr.0 system.sysDescr.0 = foo
```

SNMP Support for Routing Instances FAQs

This section presents frequently asked questions and answers related to how SNMP supports routing instances.

Can the SNMP manager access data for routing instances?

Yes, the Junos OS enables SNMP managers for all routing instances to request and manage SNMP data related to the corresponding routing instances and logical system networks.

Two different routing instance behaviors can occur, depending on where the clients originate:

- Clients from routing instances other than the default can access MIB objects and perform SNMP operations only on the logical system networks to which they belong.
- Clients from the default routing instance can access information related to all routing instances and logical system networks.

Routing instances are identified by either the context field in SNMPv3 requests or encoded in the community string in SNMPv1 or SNMPv2c requests.

When encoded in a community string, the routing instance name appears first and is separated from the actual community string by the @ character.

To avoid conflicts with valid community strings that contain the @ character, the community is parsed only if typical community string processing fails. For example, if a routing instance named **RI** is configured, an SNMP request with **RI@public** is processed within the context of the **RI** routing instance. Access control (including views, source address restrictions, and access privileges) is applied according to the actual community string (the set of data after the @ character—in this case **public**). However, if the community string **RI@public** is configured, the PDU is processed according to that community, and the embedded routing instance name is ignored.

Logical systems perform a subset of the actions of a physical router and have their own unique routing tables, interfaces, policies, and routing instances. When a routing instance is defined within a logical system, the logical system name must be encoded along with the routing instance using a slash (/) to separate the two. For example, if the routing instance **RI** is configured within the logical system **LS**, that routing instance must be encoded within a community string as **LS/RI@public**. When a routing instance is configured outside a logical system (within the default logical system), no logical system name, or **/** character, is needed.

Additionally, when a logical system is created, a default routing instance named **default** is always created within the logical system. This name should be used when querying data for that routing instance, for example **LS/default@public**. For SNMPv3 requests, the name ***logical system/routing instance*** should be identified directly in the context field.

Can I access a list of all routing instances on a device?

Yes, you can access a list of all the routing instances on a device using the vacmContextName object in the SNMP-VIEW-BASED-ACM MIB. In SNMP, each routing instance becomes a VACM context; this is why the routing instances appear in the vacmContextName object.

Can I access a default routing instance from a client in another logical router or routing instance?

No, the SNMP agent can only access data of the logical router to which it is connected.

RELATED DOCUMENTATION

SNMP Counters FAQs

This section presents frequently asked questions and answers related to SNMP counters.

Which MIB should I use for interface counters?

Interface management over SNMP is based on two tables: the **ifTable** and its extension the **ifXTable**. Both are described in RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* and RFC 2233, *The Interfaces Group MIB using SMIv2*.

Interfaces can have several layers, depending on the media, and each sublayer is represented by a separate row in the table. The relationship between the higher layer and lower layers is described in the **ifStackTable**.

The **ifTable** defines 32-bit counters for inbound and outbound octets (ifInOctets/ifOutOctets), packets (ifInUcastPkts/ifOutUcastPkts, ifInNUcastPkts /ifOutNUcastPkts), errors, and discards.

The **ifXTable** provides similar 64-bit counters, also called high capacity (HC) counters, for inbound and outbound octets (ifHCInOctets/ifHCOutOctets) and inbound packets (ifHCInUcastPkts).

When should 64-bit counters be used?

It is always good to use 64-bit counters because they contain statistics for both low and high capacity components.

Are the SNMP counters ifInOctets and ifOutOctets the same as the command reference show interfaces statistics in and out counters?

Yes, these are the same, but only if SNMP is enabled when the router boots up. If you power on a Juniper Networks device and then enable SNMP, the SNMP counters start from 0. SNMP counters do not automatically receive their statistics from the **show** command output. Similarly, using the **clear statistics** command does not clear the statistics that the SNMP counters collected, which can cause a discrepancy in the data that is seen by both processes.

Do the SNMP counters ifInOctets and ifOutOctets include the framing overhead for Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC)?

Yes.

RELATED DOCUMENTATION

Managing Traps and Informs

IN THIS SECTION

- Generating Traps Based on SysLog Events | 432
- Filtering Traps Based on the Trap Category | 433
- Filtering Traps Based on the Object Identifier | 433

The following sections contain a few tips on managing SNMP notifications:

Generating Traps Based on SysLog Events

Event policies can include an action that raises traps for events based on system log messages. This feature enables notification of an SNMP trap-based application when an important system log message occurs. You can convert any system log message, for which there is no corresponding trap, into a trap. If you are using network management system traps rather than system log messages to monitor your network, you can use this feature to ensure that you are notified of all the major events.

To configure a policy that raises a trap on receipt of an event, include the following statements at the **[edit event-options policy *policy-name*]** hierarchy level:

```
[edit event-options policy policy-name]
events [ events ];
then {
   raise-trap;
}
```

The following example shows the sample configuration for raising a trap for the event **ui_mgd_terminate**:

Generating Traps Based on SysLog Events

```
[edit event-options policy p1]
events ui_mgd_terminate;
then {
   raise-trap;
}
```

Filtering Traps Based on the Trap Category

SNMP traps are categorized into many categories. The Junos OS provides a configuration option, **categories** at the **[edit snmp trap-group *trap-group*]** hierarchy level, that enables you to specify categories of traps that you want to receive on a particular host. You can use this option when you want to monitor only specific modules of the Junos OS.

The following example shows a sample configuration for receiving only **link**, **vrrp-events**, **services**, and **otn-alarms** traps:

```
[edit snmp]
trap-group jnpr {
    categories {
        link;
        vrrp-events;
        services;
        otn-alarms;
    }
    targets {
        192.168.69.179;
    }
}
```

Filtering Traps Based on the Object Identifier

The Junos OS also provides a more advanced filter option that enables you to filter out specific traps based on their object identifiers. You can use the **notify-filter** option to filter out a specific trap or a group of traps.

The following example shows the sample configuration for excluding Juniper Networks enterprise-specific configuration management traps (note that the SNMPv3 configuration also supports filtering of SNMPv1 and SNMPv2 traps as is shown in the following example):

```
[edit snmp]
v3 {
    vacm {
        security-to-group {
            security-model v2c {
                security-name sn_v2c_trap {
                    group gr_v2c_trap;
                }
            }
        }
```

```
    access {
        group gr_v2c_trap {
            default-context-prefix {
                security-model v2c {
                    security-level none {
                        read-view all;
                        notify-view all;
                    }
                }
            }
        }
    }
}
target-address TA_v2c_trap {
    address 10.209.196.166;
    port 9001;
    tag-list tg1;
    target-parameters TP_v2c_trap;
}
target-parameters TP_v2c_trap {
    parameters {
        message-processing-model v2c;
        security-model v2c;
        security-level none;
        security-name sn_v2c_trap;
    }
    notify-filter nf1;
}
notify v2c_notify {
    type trap;
    tag tg1;
}
notify-filter nf1 {
    oid .1.3.6.1.4.1.2636.4.5 exclude;
    oid .1 include;
}
snmp-community index1 {
    community-name "$9$tDLl01h7Nbw2axN"; ## SECRET-DATA
    security-name sn_v2c_trap;
    tag tg1;
}
view all {
    oid .1 include;
}
```

```
}
```

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | 389
- Best Practices for Configuring SNMP | 558
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | 758
- Optimizing the Network Management System Configuration for the Best Results | 555
- Configuring Options on Managed Devices for Better SNMP Response Time | 556
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 643

CHAPTER 13

SNMP MIBs and Traps Supported by Junos OS

IN THIS CHAPTER

- Enterprise-Specific SNMP MIBs Supported by Junos OS | **436**
- Standard SNMP MIBs Supported by Junos OS | **452**
- Enterprise-Specific MIBs for Junos OS Evolved on PTX10003 Devices | **479**
- Standard MIBs for Junos OS Evolved on PTX10003 Devices | **482**
- Standard SNMP Traps Supported by Junos OS | **490**
- Enterprise-Specific SNMP Traps Supported by Junos OS | **500**
- Customized SNMP MIBs for Syslog Traps | **521**
- Example Custom Syslog Trap | **537**

Enterprise-Specific SNMP MIBs Supported by Junos OS

Junos OS supports the enterprise-specific MIBs listed in Table 29 on page 436. For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer.

Table 29: Enterprise-specific MIBs supported by Junos OS

Enterprise-Specific MIB	Description	Platforms
AAA Objects MIB	Provides support for monitoring user authentication, authorization, and accounting through the RADIUS, LDAP, SecurID, and local authentication servers.	SRX Series and vSRX
Access Authentication Objects MIB	Provides support for monitoring firewall authentication, including data about the users trying to access firewall-protected resources and the firewall authentication service itself.	SRX Series and vSRX

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Alarm MIB	Provides information about alarms from the router chassis.	All platforms
Analyzer MIB	Provides information about analyzer and remote analyzer related to port mirroring on the EX Series Ethernet Switches. Port mirroring is a method used on enterprise switches to monitor and analyze traffic on the network. When port mirroring is enabled, copies of all (or a sample set of) packets are forwarded from one port of the switch to another port on the same switch (analyzer) or on another switch (remote analyzer) where the packet can be analyzed and studied.	EX Series, QFabric system, and QFX Series
Antivirus Objects MIB	Provides information about the antivirus engine, antivirus scans, and antivirus scan-related traps.	SRX Series and vSRX
ATM Class-of-Service MIB	Provides support for ATM interfaces and virtual connections.	ACX Series, M Series, and T Series
ATM MIB	Provides support for monitoring Asynchronous Transfer Mode, version 2 (ATM2) virtual circuit (VC) class-of-service (CoS) configurations. It also provides CoS queue statistics for all VCs that have CoS configured.	M Series, SRX Series, T Series and vSRX
BGP4 V2 MIB	Provides support for monitoring BGP peer-received prefix counters. It is based upon similar objects in the MIB documented in Internet draft draft-ietf-idr-bgp4-mibv2-03.txt, *Definitions of Managed Objects for the Fourth Version of BGP (BGP-4), Second Version*.	All platforms

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Bidirectional Forwarding Detection MIB	Provides support for monitoring Bidirectional Forwarding Detection (BFD) sessions.	All platforms
Chassis Cluster MIB	Provides information about objects that are used whenever the state of the control link interfaces or fabric link interfaces changes (up to down or down to up) in a chassis cluster deployment.	SRX Series and vSRX
Chassis Definitions for Router Model MIB	Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify platform and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often.	ACX Series, M Series, MX Series, PTX Series, QFX Series, SRX550, SRX1500, and T Series
Chassis MIBs	Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and air flow) and inventory support for the chassis, System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), Switch Fabric Board (SFB), Flexible PIC Concentrators (FPCs), and PICs.	All platforms
Class-of-Service MIB	Provides support for monitoring interface output queue statistics per interface and per forwarding class.	ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric system, QFX Series, SRX Series, T Series, and vSRX

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Configuration Management MIB	Provides notification for configuration changes as SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in **jnxCmChgEventTable**.	All platforms
Destination Class Usage MIB	Provides support for monitoring packet counts based on the ingress and egress points for traffic transiting your networks. Ingress points are identified by the input interface. Egress points are identified by destination prefixes grouped into one or more sets, known as destination classes. One counter is managed per interface per destination class, up to a maximum of 16 counters per interface.	EX Series, M Series, SRX Series, T Series, and vSRX
DHCP MIB	Provides SNMP support (get and trap) for DHCP local server and relay configurations. It also provides support for bindings and leases tables, and for statistics.	M Series, MX Series, and T Series
DHCPv6 MIB	Provides SNMP support (get and trap) for DHCPv6 local server and relay configurations. It also provides support for bindings and leases tables, and for statistics.	M Series, MX Series, and T Series
Digital Optical Monitoring MIB	Provides support for the **SNMP Get** request for statistics and **SNMP Trap** notifications for alarms.	EX Series, M Series, MX Series, PTX Series, and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
DNS Objects MIB	Provides support for monitoring DNS proxy queries, requests, responses, and failures.	SRX Series and vSRX
Dynamic Flow Capture MIB	Provides support for monitoring the operational status of dynamic flow capture (DFC) PICs.	M Series and T Series
Ethernet MAC MIB	Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, **inoctets**, **inframes**, **outoctets**, and **outframes** on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port.	EX Series, M Series, MX Series, QFX Series, SRX300, SRX320, SRX340, SRX550, SRX1500 and T Series
Event MIB	Defines a generic trap that can be generated using an op script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found.	ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric system, QFX Series, SRX1500, SRX300, SRX320, SRX340, SRX550, and T Series
Experimental MIB	Contains object identifiers for experimental MIBs.	ACX Series, M series, MX Series, and T series
EX Series MAC Notification MIB	Contains Juniper Networks' implementation of enterprise-specific MIB for Ethernet Mac Stats for EX Series.	EX Series
EX Series SMI MIB	Contains the Structure of Management Information for Juniper Networks EX Series platforms.	EX Series
Firewall MIB	Provides support for monitoring firewall filter counters. Routers must have the Internet Processor II ASIC to perform firewall monitoring.	ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric system, QFX Series, SRX300, SRX320, SRX340, SRX550, SRX1500 and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Flow Collection Services MIB	Provides statistics on files, records, memory, FTP, and error states of a monitoring services interface. It also provides SNMP traps for unavailable destinations, unsuccessful file transfers, flow overloading, and memory overloading.	M Series and T Series
GRE Keepalive Monitoring MIB	Provides support for monitoring generic routing encapsulation (GRE) keepalive status. This MIB also provides an SNMP trap when GRE keepalive status changes.	SRX Series and vSRX instances
Host Resources MIB	Extends the **hrStorageTable** object, providing a measure of the usage of each file system on the router in percentage format. Previously, the objects in the **hrStorageTable** measured the usage in allocation units—**hrStorageUsed** and **hrStorageAllocationUnits**—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.	ACX Series, EX Series, M Series, MX Series, QFX Series, SRX300, SRX320, SRX340, SRX550, SRX1500 and T Series
Interface Accounting Forwarding Class MIB	Extends the Juniper Enterprise Interface MIB and provides support for monitoring statistics data for interface accounting and IETF standardization.	M Series, MX Series, SRX Series, and vSRX
Interface MIB	Extends the standard **ifTable** (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information.	ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric system, QFX Series, SRX300, SRX320, SRX340, SRX550, SRX1500 and T Series
IP Forward MIB	Extends the standard IP Forwarding Table MIB (RFC 4292) to include CIDR forwarding information.	All platforms

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
IPsec Generic Flow Monitoring Object MIB	Based on **jnx-ipsec-monitor-mib**, this MIB provides support for monitoring IPsec and IPsec VPN management objects.	SRX Series and vSRX
IPsec Monitoring MIB	Provides operational and statistical information related to the IPsec and IKE tunnels on Juniper Networks routers.	M Series, SRX Series, and T Series
IPsec VPN Objects MIB	Provides support for monitoring IPsec and IPsec VPN management objects for Juniper products. This MIB is an extension of **jnx-ipsec-flow-mon.mib**.	SRX Series and MX Series with USF
IPv4 MIB	Provides additional Internet Protocol version 4 (IPv4) address information, supporting the assignment of identical IPv4 addresses to separate interfaces.	All platforms
IPv6 and ICMPv6 MIB	Provides IPv6 and Internet Control Message Protocol version 6 (ICMPv6) statistics.	M series, MX Series, PTX Series, SRX Series, T Series, and vSRX
jnxJsFlowSofSummary MIB	Provides the total number of Express Path mode (formerly known as services offloading) sessions in use and total number of packets processed so far in logical system.	SRX4600, SRX5400, SRX5600, and SRX5800.
jnxUserFirewalls MIB	Exports statistics of User Firewall identity-management counters.	SRX Series and vSRX
jnxTLBMIB	Exports statistics of Traffic Load Balancer application	MX240, MX480, and MX960

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
L2ALD MIB	Contains information about the Layer 2 Address Learning Daemon (L2ALD) and related traps, such as the routing instance MAC limit trap and the interface MAC limit trap. This MIB also provides VLAN information in the **jnxL2aldVlanTable** table for Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches. **NOTE:** Non-ELS EX Series switches support the VLAN MIB (**jnxExVlanTable** table) for VLAN information instead of this MIB. See the SNMP MIB Explorer.	EX Series, MX Series, QFX Series, and T Series
L2CP MIB	Provides information about Layer 2 Control Protocols (L2CP) based features. Currently, Junos OS supports only the **jnxDot1dStpPortRootProtectEnabled**, **jnxDot1dStpPortRootProtectState**, and **jnxPortRootProtectStateChangeTrap** objects.	MX Series
L2TP MIB	Provides information about Layer 2 Transport Protocol (L2TP) tunnels and sessions.	M Series, MX Series, and T Series
LDP MIB	Provides LDP statistics and defines LDP label-switched path (LSP) notifications. LDP traps support only IPv4 standards.	ACX Series, M Series, PTX Series, SRX Series, and T Series
License MIB	Extends SNMP support to licensing information, and introduces SNMP traps that alert users when the licenses are about to expire, expire, or when the total number of users exceeds the number specified in the license.	M Series, MX Series, SRX Series, and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Logical Systems MIB	Extend SNMP support to logical systems security profile through various MIBs defined under **jnxLsysSecurityProfile**.	SRX Series
LTE MIB	Extend SNMP support to monitor the 4G LTE Mini-Physical Interface Module (Mini-PIM) status using SNMP remote network management.	SRX300, SRX320, SRX340, SRX345, and SRX550M.
MIMSTP MIB	Provides information about MSTP instances (that is, routing instances of type Virtual Switch/Layer 2 control, also known as virtual contexts), MSTIs within the MSTP instance, and VLANs associated with the MSTI.	MX Series and T Series
MPLS LDP MIB	Contains object definitions as described in RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*. **NOTE:** Objects in the MPLS LDP MIB were supported in earlier releases of Junos OS as a proprietary LDP MIB (**mib-ldpmib.txt**). Because the branch used by the proprietary LDP (**mib-ldpmib.txt**) conflicts with RFC 3812, the proprietary LDP MIB (**mib-ldpmib.txt**) has been deprecated and replaced by the enterprise-specific MPLS LDP MIB (**mib-jnx-mpls-ldp.txt**).	ACX Series, EX Series, M Series, MX Series, PTX Series, QFX Series, and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
MPLS MIB	Provides MPLS information and defines MPLS notifications. **NOTE:** To collect information about MPLS statistics on transit routers, use the enterprise-specific RSVP MIB (**mib-jnx-rsvp.txt**) instead of the enterprise-specific MPLS MIB (**mib-jnx-mpls.txt**).	ACX Series, EX Series, M Series, MX Series, PTX Series, QFX Series, SRX Series, and T Series
MVPN MIB	Contains objects that enable SNMP manager to monitor MVPN connections on the provider edge routers. The enterprise-specific MVPN MIB is the Juniper Networks extension of the IETF standard MIBs defined in Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*.	All platforms
NAT Objects MIB	Provides support for monitoring network address translation (NAT). .	EX Series and SRX Series
NAT Resources-Monitoring MIB	Provides support for monitoring NAT pools usage and NAT rules. Notifications of usage of NAT resources are also provided by this MIB. This MIB is currently supported on the Multiservices PIC and Multiservices DPC on M Series and MX Series routers only.	M Series and MX Series
OTN Interface Management MIB	Defines objects for managing Optical Transport Network (OTN) interfaces on devices running Junos OS.	M Series, MX series, PTX Series, and T Series
Packet Forwarding Engine MIB	Provides notification statistics for Packet Forwarding Engines.	ACX Series, EX Series, M Series, PTX Series, SRX Series, and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Packet Mirror MIB	Enables you to capture and view packet mirroring-related information. This MIB is currently supported by Junos OS for MX Series routers only. Packet mirroring traps are an extension of the standard SNMP implementation and are only available to SNMPv3 users.	MX Series
PAE Extension MIB	Extends the standard IEEE802.1x PAE Extension MIB, and contains information for Static MAC Authentication.	EX Series
Passive Monitoring MIB	Performs traffic flow monitoring and lawful interception of packets transiting between two routers.	M Series and T Series
Ping MIB	Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in **pingCtlTable** of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB.	ACX Series, EX Series, M Series, MX Series, QFX Series, SRX Series, and T Series
Policy Objects MIB	Provides support for monitoring the security policies that control the flow of traffic from one zone to another.	SRX Series
Power Supply Unit MIB	Enables monitoring and managing of the power supply on a device running Junos OS.	EX Series and QFabric system
PPP MIB	Provides SNMP support for PPP-related information such as the type of authentication used, interface characteristics, status, and statistics. This MIB is supported on Common Edge PPP process, jpppd.	M Series and MX Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
PPPoE MIB	Provides SNMP support for PPPoE-related information such as the type of authentication used, interface characteristics, status, and statistics. This MIB is supported on Common Edge PPPoE process, jpppoed.	M Series and MX Series
Pseudowire ATM MIB	Extends the standard Pseudowire MIB, and defines objects used for managing the ATM pseudowires in Juniper products. The enterprise-specific Pseudowire ATM MIB is the Juniper Networks implementation of RFC 5605, *Managed Objects for ATM over Packet Switched Networks (PSNs)*.	M Series and MX Series
Pseudowire TDM MIB	Extends the standard Pseudowire MIB, and contains information about configuration and statistics for specific pseudowire types. The enterprise-specific Pseudowire TDM MIB is the Juniper Networks implementation of the standard Managed Objects for TDM over Packet Switched Network MIB (draft-ietf-pwe3-tdm-mib-08.txt).	ACX Series, M Series, and T Series
PTP MIB	Monitors the operation of PTP clocks within the network.	MX Series
Real-Time Performance Monitoring MIB	Provides real-time performance-related data and enables you to access jitter measurements and calculations using SNMP.	EX Series, M Series, MX Series, SRX Series, and T Series
Reverse-Path-Forwarding MIB	Monitors statistics for traffic that is rejected because of reverse-path-forwarding (RPF) processing.	All platforms

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
RMON Events and Alarms MIB	Supports the Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments **alarmTable** with additional information about each alarm. Two new traps are also defined to indicate when problems are encountered with an alarm.	All platforms
RSVP MIB	Provides information about RSVP-traffic engineering sessions that correspond to MPLS LSPs on transit routers in the service provider core network. **NOTE:** To collect information about MPLS statistics on transit routers, use the enterprise-specific RSVP MIB (**mib-jnx-rsvp.txt**) instead of the enterprise-specific MPLS MIB (**mib-jnx-mpls.txt**).	ACX Series, M Series, MX Series, PTX Series, and T Series
Security Interface Extension Objects MIB	Provides support for the security management of interfaces.	EX Series, SRX Series, and vSRX
Security Screening Objects MIB	Defines the MIB for the Juniper Networks Enterprise Firewall screen functionality.	SRX Series and vSRX
Services PIC MIB	Provides statistics for Adaptive Services (AS) PICs and defines notifications for AS PICs.	M Series and T Series
SNMP IDP MIB	Contains Juniper Networks' implementation of enterprise specific MIB for IDP.	SRX Series and vSRX
SONET APS MIB	Monitors any SONET interface that participates in Automatic Protection Switching (APS).	M Series and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
SONET/SDH Interface Management MIB	Monitors the current alarm for each SONET/SDH interface.	M Series and T Series
Source Class Usage MIB	Counts packets sent to customers by performing a lookup on the IP source address and the IP destination address. The Source Class Usage (SCU) MIB makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge.	M Series, T Series, and SRX Series
SPU Monitoring MIB	Provides support for monitoring SPUs on SRX5600 and SRX5800 devices.	SRX Series and vSRX
Structure of Management Information MIB	Explains how the Juniper Networks enterprise-specific MIBs are structured.	ACX Series, EX Series, M Series, MX series, QFX Series, SRX Series, T Series and vSRX
Structure of Management Information MIB for EX Series Ethernet Switches	Defines a MIB branch for switching-related MIB definitions for the EX Series Ethernet Switches.	EX Series
Structure of Management Information MIB for SRX Series	Contains object identifiers (OIDs) for the security branch of the MIBs used in Junos OS for SRX Series devices, services, and traps.	SRX Series and vSRX
Subscriber MIB	Provides SNMP support for subscriber-related information.	ACX Series, MX Series, and T Series
System Log MIB	Enables notification of an SNMP trap-based application when an important system log message occurs.	EX Series, M Series, MX Series, PTX Series, QFX Series, SRX Series, and T Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
Traceroute MIB	Supports the Junos OS extensions of traceroute and remote operations. Items in this MIB are created when entries are created in the **traceRouteCtlTable** of the Traceroute MIB. Each item is indexed exactly the same way as it is in the Traceroute MIB.	EX Series, M Series, MX Series, SRX Series, T Series, and vSRX
Tunnel Stats MIB	Supports monitoring of tunnel statistics for IPV4 over IPV6 tunnels. This MIB currently displays three counters: tunnel count in rpd, tunnel count in Kernel, and tunnel count in the Packet Forwarding Engine.	all platforms
Utility MIB	Provides SNMP support for exposing the Junos OS data and has tables that contain information about each type of data, such as integer and string.	EX Series, M Series, MX Series, QFabric system, QFX Series, SRX Series, T Series, and vSRX
Virtual Chassis MIB	Contains information about the virtual chassis on the EX Series Ethernet Switches and the MX Series.	EX Series and MX Series
VLAN MIB	Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients. **NOTE:** For ELS EX Series switches and QFX Series switches, VLAN information is provided in the L2ALD MIB in the **jnxL2aldVlanTable** table instead of in this MIB. See theSNMP MIB Explorer for details. Non-ELS EX Series Ethernet switches use the **jnxExVlanTable** table in this MIB to provide VLAN configuration information, and the **jnxVlanTable** table in this MIB has been deprecated and is no longer used.	EX Series and QFX Series

Table 29: Enterprise-specific MIBs supported by Junos OS *(continued)*

Enterprise-Specific MIB	Description	Platforms
VPLS MIBs	Provides information about generic, BGP-based, and LDP-based VPLS, and pseudowires associated with the VPLS networks. The enterprise-specific VPLS MIBs are Juniper Networks extensions of the following IETF standard MIBs defined in Internet draft draft-ietf-l2vpn-vpls-mib-05.txt, and are implemented as part of the **jnxExperiment** branch: • **VPLS-Generic-Draft-01-MIB** implemented as **mib-jnx-vpls-generic.txt** • **VPLS-BGP-Draft-01-MIB** implemented as **mib-jnx-vpls-bgp.txt** • **VPLS-LDP-Draft-01-MIB** implemented as **mib-jnx-vpls-ldp.txt**	M Series, MX Series, and T Series
VPN Certificate Objects MIB	Provides support for monitoring the local and CA certificates loaded on the router.	EX Series, SRX Series, and vSRX
VPN MIB	Provides monitoring for Layer 3 VPNs, Layer 2 VPNs, and virtual private LAN service (VPLS) (read access only).	ACX Series, EX Series, M Series, MX Series, and T Series

Starting in Junos OS Release 18.4R1, you can monitor 4G LTE Mini-PIM status by using SNMP remote network management.

You can use the following commands to monitor the 4G LTE Mini-PIM status:

show snmp mib walk ascii jnxWirelessWANNetworkInfoTable

show snmp mib walk ascii jnxWirelessWANFirmwareInfoTable

In previous releases, the **show modem wireless network interface *interface-name*** and **show modem wireless firmware interface *interface-name*** commands are used to check the 4G LTE Mini-PIM status.

Starting in Junos OS Release 19.4R1, on SRX5000 Series devices with SRX5K-SPC3 card, we have enhanced the existing IPsec VPN flow monitor MIB **jnxIpSecFlowMonMIB** to support the global IKE statistics for tunnels using IKEv2. Use the **show security ike stats** command to display the global statistics of tunnels such as in-progress, established, and expired negotiations using IKEv2.

Starting in Junos OS Release 20.1R1, you can enable the peer down and IPsec tunnel down traps and configure the certificate authority (CA) and local certificate traps. We've enhanced the existing IPsec VPN flow monitor MIB **jnxIpSecFlowMonMIB** to support the global data plane, active IKE SA, active IPsec SA, and active peer statistics for tunnels using IKEv2. We've also enhanced the output of the **show security ike stats** command to add additional options **(<brief> | <detail>)**. Use the **clear security ike stats** command to clear the IKEv2 statistic counters.

For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer.

RELATED DOCUMENTATION

Network Management and Monitoring Guide

Standard SNMP MIBs Supported by Junos OS | **452**

Enterprise-Specific SNMP Traps Supported by Junos OS | **500**

Standard SNMP MIBs Supported by Junos OS

Junos OS supports the Standard MIBs listed in Table 30 on page 452.

> **NOTE:** For details on SNMP MIB support on EX4600 switches, QFX Series switches, and QFabric systems, see "SNMP MIBs Support" on page 616.

Table 30: Standard MIBs supported by Junos OS

Standard MIB	Exceptions	Platforms
IEEE 802.1ab section 12.1, *Link Layer Discovery Protocol (LLDP) MIB*	EX Series implementation of LLDP MIB supports both IPv4 and IPv6 configuration.	EX Series and MX Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
IEEE, 802.3ad, *Aggregation of Multiple Link Segments*	Supported tables and objects: • **dot3adAggPortTable**, **dot3adAggPortListTable**, **dot3adAggTable**, and **dot3adAggPortStatsTable** **NOTE:** EX Series switches do not support the **dot3adAggPortTable** and **dot3adAggPortStatsTable**. • **dot3adAggPortDebugTable** (only **dot3adAggPortDebugRxState**, **dot3adAggPortDebugMuxState**, **dot3adAggPortDebugActorSyncTransitionCount**, **dot3adAggPortDebugPartnerSyncTransitionCount**, **dot3adAggPortDebugActorChangeCount**, and **dot3adAggPortDebugPartnerChangeCount**) **NOTE:** EX Series switches do not support the **dot3adAggPortDebugTable**. • **dot3adTablesLastChanged**	EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, and vSRX

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
IEEE, 802.1ag, *Connectivity Fault Management*	Supported tables and objects: • **dot1agCfmMdTableNextIndex** • **dot1agCfmMdTable** (except **dot1agCfmMdMhfIdPermission**) • **dot1agCfmMaNetTable** • **dot1agCfmMaMepListTable** • **dot1agCfmDefaultMdDefLevel** • **dot1agCfmDefaultMdDefMhfCreation** • **dot1agCfmMepTable** (except **dot1agCfmMepLbrBadMsdu**, **dot1agCfmMepTransmitLbmVlanPriority**, **dot1agCfmMepTransmitLbmVlanDropEnable**, **dot1agCfmMepTransmitLtmFlags**, **dot1agCfmMepPbbTeCanReportPbbTePresence**, **dot1agCfmMepPbbTeTrafficMismatchDefect**, **dot1agCfmMepPbbTransmitLbmLtmReverseVid**, **dot1agCfmMepPbbTeMismatchAlarm**, **dot1agCfmMepPbbTeLocalMismatchDefect**, and **dot1agCfmMepPbbTeMismatchSinceReset**) • **dot1agCfmLtrTable** (except **dot1agCfmLtrChassisIdSubtype**, **dot1agCfmLtrChassisId**, **dot1agCfmLtrManAddressDomain**, **dot1agCfmLtrManAddress**, **dot1agCfmLtrIngressPortIdSubtype**, **dot1agCfmLtrIngressPortId**, **dot1agCfmLtrEgressPortIdSubtype**, **dot1agCfmLtrEgressPortId**, and **dot1agCfmLtrOrganizationSpecificTlv**) • **dot1agCfmMepDbTable** (except **dot1agCfmMebDbChassisIdSubtype**, **dot1agCfmMebDbChassisId**, **dot1agCfmMebDbManAddressDomain**, and **dot1agCfmMebDbManAddress**)	EX Series, MX Series, PTX Series, and QFX Series
IEEE, 802.1ap, *Management Information Base (MIB) definitions for VLAN Bridges*	Supported tables and objects: • **ieee8021CfmStackTable** • **ieee8021CfmVlanTable** • **ieee8021CfmDefaultMdTable** (except **ieee8021CfmDefaultMdIdPermission**) • **ieee8021CfmMaCompTable** (except **ieee8021CfmMaCompIdPermission**)	MX Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*	No exceptions	All platforms
RFC 1157, *A Simple Network Management Protocol (SNMP)*	No exceptions	All platforms
RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*	Supported tables and objects: • **isisSystem** • **isisMANAreaAddr** • **isisAreaAddr** • **isisSysProtSupp** • **isisSummAddr** • **isisCirc** • **isisCircLevel** • **isisPacketCount** • **isisISAdj** • **isisISAdjAreaAddr** • **isisAdjIPAddr** • **isisISAdjProtSupp** • **isisRa** • **isisIPRA**	All platforms
RFC 1212, *Concise MIB Definitions*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	Junos OS supports the following areas:
	• MIB II and its SNMP version 2 derivatives, including:
	  ◦ Statistics counters
	  ◦ IP, except for **ipRouteTable**, which has been replaced by **ipCidrRouteTable** (RFC 2096, *IP Forwarding Table MIB*)
	  ◦ SNMP management
	  ◦ Interface management
	• SNMPv1 **Get**, **GetNext** requests, and version 2 **GetBulk** request
	• Junos OS-specific secured access list
	• Master configuration keywords
	• Reconfigurations upon SIGHUP
		ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

RFC 1215, *A Convention for Defining Traps for use with the SNMP*	Junos OS supports only MIB II SNMP version 1 traps and version 2 notifications.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*	Junos OS supports T1 MIB.	ACX Series, M Series, SRX Series, and T Series
RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type*	Junos OS supports T3 MIB.	M Series and T Series
RFC 1471, *Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol*	Supported tables and objects: • **pppLcp 1** object • **pppLinkStatustable** table • **pppLinkConfigTable** table	M Series, MX Series, and PTX Series
RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 1695, *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2*	No exceptions	ACX Series, M Series, PTX Series, and T Series
RFC 1850, *OSPF Version 2 Management Information Base*	Unsupported tables, objects, and traps: • **ospfOriginateNewLsas** object • **ospfRxNewLsas** object • The host table • **ospfOriginateLSA** trap **ospfLsdbOverflow** trap **ospfLsdbApproachingOverflow** trap	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 1901, *Introduction to Community-based SNMPv2*	No exceptions	All platforms
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, and T Series
RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2024, *Definitions of Managed Objects for Data Link Switching Using SMIv2*	Unsupported tables, objects, and traps with read-only access: • **dlswInterface** object group **dlswSdlc** object group **dlswDirLocateMacTable** table **dlswDirNBTable**table **dlswDirLocateNBTable** table **dlswCircuitDiscReasonLocal** tabular object **dlswCircuitDiscReasonRemote** tabular object **dlswDirMacCacheNextIndex** scalar object **dlswDirNBCacheNextIndex** scalar object	M Series, MX Series, and T Series
RFC 2096, *IP Forwarding Table MIB* **NOTE:** RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.	The **ipCidrRouteTable** has been extended to include the tunnel name when the next hop is through an RSVP-signaled LSP.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*	Unsupported table and objects: • **frCircuitTable** • **frErrTable**	M Series, MX Series, SRX Series, and T Series
RFC 2233, *The Interfaces Group MIB Using SMIv2* **NOTE:** RFC 2233 has been replaced by RFC 2863, IF MIB. However, Junos OS supports both RFC 2233 and RFC 2863.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2287, *Definitions of System-Level Managed Objects for Applications*	Supported tables and objects: • **sysApplInstallPkgTable** • **sysApplInstallElmtTable** • **sysApplElmtRunTable** • **sysApplMapTable**	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except for IPv6 interface statistics)	Junos OS does not support IPv6 interface statistics.	ACX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*	Unsupported tables, objects, and traps: • **dsx1FarEndConfigTable** • **dsx1FarEndCurrentTable** • **dsx1FarEndIntervalTable** • **dsx1FarEndTotalTable** • **dsx1FracTable**	ACX Series, M Series, SRX Series, and T Series
RFC 2515, *Definitions of Managed Objects for ATM Management*	Unsupported table and objects: • **atmVpCrossConnectTable** • **atmVcCrossConnectTable** • **aal5VccTable**	ACX Series, M Series, and T Series
RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access) **NOTE:** RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access) **NOTE:** RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* **NOTE:** RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2579, *Textual Conventions for SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2580, *Conformance Statements for SMIv2*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2662, *Definitions of Managed Objects for ADSL Lines*	No exceptions	M Series, MX Series, SRX Series, and T Series
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types* **NOTE:** The list of managed objects specified in RFC 2665 has been updated by RFC 3635 by including information useful for the management of 10-Gigabit per second Ethernet interfaces.	For M Series, T Series, and MX Series, the SNMP counters do not count the Ethernet header and frame check sequence (FCS). Therefore, the Ethernet header bytes and the FCS bytes are not included in the following four tables: • **ifInOctets** • **ifOutOctets** • **ifHCInOctets** • **ifHCOutOctets** However, the EX switches adhere to RFC 2665.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	Unsupported table and objects: • **vrrpStatsPacketLengthErrors** **NOTE:** Junos OS does not support this standard for row creation and the **Set** operation.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2790, *Host Resources MIB*	Supported tables and objects: • **hrStorageTable** **NOTE:** The file systems **/**, **/config**, **/var**, and **/tmp** always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change. • **hrSystem** group • **hrSWInstalled** group • **hrProcessorTable**	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2819, *Remote Network Monitoring Management Information Base*	Supported tables and objects: • **etherStatsTable** (for Ethernet interfaces only), **alarmTable**, **eventTable**, and **logTable** are supported on all devices running Junos OS. • **historyControlTable** and **etherHistoryTable** (except **etherHistoryUtilization** object) are supported only on EX Series switches.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2863, *The Interfaces Group MIB* **NOTE:** RFC 2863 replaces RFC 2233. However, Junos OS supports both RFC 2233 and RFC 2863.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*	No exceptions	M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2922, *The Physical Topology (PTOPO) MIB*	Supported objects: • **ptopoConnDiscAlgorithm** • **ptopoConnAgentNetAddrType** • **ptopoConnAgentNetAddr** • **ptopoConnMultiMacSASeen** • **ptopoConnMultiNetSASeen** • **ptopoConnIsStatic** • **ptopoConnLastVerifyTime** • **ptopoConnRowStatus**	EX Series and SRX Series
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	Supported tables and objects: • **pingCtlTable** • **pingResultsTable** • **pingProbeHistoryTable** • **pingMaxConcurrentRequests** • **traceRouteCtlTable** • **traceRouteResultsTable** • **traceRouteProbeHistoryTable** • **traceRouteHopsTable**	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 2932, *IPv4 Multicast Routing MIB*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2934, *Protocol Independent Multicast MIB for IPv4* **NOTE:** In Junos OS, RFC 2934 is implemented based on a draft version, *pimmib.mib*, of the now standard RFC.	Support for the **pimNeighborLoss** trap was added in Release 11.4.	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 2981, *Event MIB*	No exceptions	ACX Series, M Series, MX Series, PTX Series, and T Series
RFC 3014, *Notification Log MIB*	No exceptions	ACX Series, M Series, MX Series, PTX Series, and T Series
RFC 3019, *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*	No exceptions	M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* **NOTE:** RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* **NOTE:** RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3413, *Simple Network Management Protocol (SNMP) Applications*	Unsupported tables and objects: • Proxy MIB	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, L3VPN MIB **NOTE:** RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)* **NOTE:** RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures* (implemented under the Juniper Networks enterprise branch [**jnxExperiment**])	No exceptions	M Series and T Series
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 3591 *Managed Objects for the Optical Interface Type*	Supported tables and objects: • **optIfOTMnTable** (except **optIfOTMnOpticalReach**, **optIfOTMnInterfaceType**, and **optIfOTMnOrder**) • **optIfOChConfigTable** (except **optIfOChDirectionality** and **optIfOChCurrentStatus**) • **optIfOTUkConfigTable** (except **optIfOTUkTraceIdentifierAccepted**, **optIfOTUkTIMDetMode**, **optIfOTUkTIMActEnabled**, **optIfOTUkTraceIdentifierTransmitted**, **optIfOTUkDEGThr**, **optIfOTUkDEGM**, **optIfOTUkSinkAdaptActive**, and **optIfOTUkSourceAdaptActive**) • **optIfODUkConfigTable** (except **optIfODUkPositionSeqCurrentSize** and **optIfODUkTtpPresent**)	M Series, MX Series, PTX Series, and T Series
RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*	No exceptions	M Series, MX Series, and T Series
RFC 3621, *Power Ethernet MIB*	No exceptions	EX Series
RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*	Unsupported tables and objects: • **dot3StatsRateControlAbility** • **dot3StatsRateControlStatus** in **dot3StatsEntry** table **NOTE:** The values of the following objects in **dot3HCStatsEntry** table will be always zero for both 32-bit counters and 64-bit counters: • **dot3HCStatsSymbolErrors** • **dotHCStatsInternalMacTransmitErrors**	MX Series
RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*	Unsupported tables and objects: • **etherWisDeviceTable**, • **etherWisSectionCurrentTable** • **etherWisFarEndPathCurrentTable**	M Series, MX Series, PTX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 3811, *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*	No exceptions	ACX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)* (read-only access)	MPLS tunnels as interfaces are not supported. **mplsTunnelCHopTable** is supported on ingress routers only. **NOTE:** The branch used by the proprietary LDP MIB (**ldpmib.mib**) conflicts with RFC 3812. **ldpmib.mib** has been deprecated and replaced by **jnx-mpls-ldp.mib**. Unsupported tables and objects: • **mplsTunnelResourceMeanRate** in **TunnelResource** table • **mplsTunnelResourceMaxBurstSize** in **TunnelResource** table • **mplsTunnelResourceMeanBurstSize** in **TunnelResource** table • **mplsTunnelResourceExBurstSize** in **TunnelResource** table • **mplsTunnelResourceWeight** in **TunnelResource** table • **mplsTunnelPerfTable** • **mplsTunnelCRLDPResTable**	ACX Series, M Series, MX Series, PTX Series, and T Series
RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*	Unsupported tables and objects (read-only access): • **mplsInterfacePerfTable** • **mplsInSegmentPerfTable** • **mplsOutSegmentPerfTable** • **mplsInSegmentMapTable** • **mplsXCUp** • **mplsXCDown**	ACX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 3877, *Alarm Management Information Base*	• Junos OS does not support the **alarmActiveStatsTable.** • Traps that do not conform to the alarm model are not supported. However, these traps can be redefined to conform to the alarm model.	MX Series
RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*	Unsupported tables and objects: • **dsx3FarEndConfigTable** • **dsx3FarEndCurrentTable** • **dsx3FarEndIntervalTable** • **dsx3FarEndTotalTable** • **dsx3FracTable**	M Series and T Series
RFC 4087, *IP Tunnel MIB*	Describes MIB objects in the following tables for managing tunnels of any type over IPv4 and IPv6 networks: • **tunnelIfTable**—Provides information about the tunnels known to a router. • **tunnelInetConfigTable**—Assists dynamic creation of tunnels and provides mapping from end-point addresses to the current interface index value. **NOTE:** Junos OS supports **MAX-ACCESS** of read-only for all the MIB objects in **tunnelIfTable** and **tunnelInetConfigTable** tables.	M Series, MX Series, and T Series
RFC 4133, *Entity MIB*	Unsupported tables and objects: • **entityLogicalGroup** table • **entPhysicalMfgDate** and **entPhysicalUris** objects in **entityPhysical2Group** table • **entLPMappingTable** and **entPhysicalContainsTable** in **entityMappingGroup** table • **entityNotoficationsGroup** table	Only MX240, MX480, and MX960 routers, and EX2200 and EX3300 switches

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms

RFC 4188, *Definitions of Managed Objects for Bridges*	• Supports 802.1D STP(1998)
	• Supported subtrees and objects:
	  ◦ **dot1dStp** subtree is supported on MX Series 5G Universal Routing Platforms.
	  ◦ **dot1dTpFdbAddress**, **dot1dTpFdbPort**, and **dot1dTpFdbStatus** objects from the **dot1dTpFdbTable** of the **dot1dTp** subtree are supported on EX Series Ethernet Switches.
	  ◦ **dot1dTpLearnedEntryDiscards** and **dot1dTpAgingTime** objects are supported on M Series and T Series routers.
		MX Series, EX Series, and M Series and T Series

RFC 4268, *Entity State MIB*	No exceptions	Only MX240, MX480, and MX960 routers, and EX2200 and EX3300 switches
RFC 4273, *Definitions of Managed Objects for BGP-4*	Supported tables and objects: • **jnxBgpM2PrefixInPrefixesAccepted** • **jnxBgpM2PrefixInPrefixesRejected**	ACX Series, EX Series, M Series, MX Series, SRX Series, and T Series
RFC 4292, *IP Forwarding MIB*	Supported tables and objects: • **inetCidrRouteTable** • **inetCidrRouteNumber** • **inetCidrRouteDiscards** **NOTE:** Junos OS currently supports these MIB objects that will be deprecated in future releases: **ipCidrRouteTable**, **ipCidrRouteNumber**, and **ipCidrRouteDiscards**.	ACX Series, EX Series, M Series, MX Series, PTX Series, and T Series
RFC 4293, *Management Information Base for the Internet Protocol (IP)*	Supports only the mandatory groups.	MX Series and EX Series
RFC 4318, *Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol*	Supports 802.1w and 802.1t extensions for RSTP.	EX Series, M Series, MX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 4363b, *Q-Bridge VLAN MIB*	No exceptions	MX Series and EX Series
RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB*	Supported tables and objects: • **mplsL3VpnActiveVrfs** • **mplsL3VpnConfiguredVrfs** • **mplsL3VpnConnectedInterfaces** • **mplsL3VpnVrfConfMidRteThresh** • **mplsL3VpnVrfConfHighRteThresh** • **mplsL3VpnIfConfRowStatus** • **mplsL3VpnIllLblRcvThrsh** • **mplsL3VpnNotificationEnable** • **mplsL3VpnVrfConfMaxPossRts** • **mplsL3VpnVrfConfRteMxThrshTime** • **mplsL3VpnVrfOperStatus** • **mplsL3VpnVrfPerfCurrNumRoutes** • **mplsL3VpnVrfPerfTable** • **mplsL3VpnVrfRteTable** • **mplsVpnVrfRTTable** • **mplsL3VpnVrfTable** • **mplsL3VpnIfConfTable**	EX Series, M Series, MX Series, PTX Series, and T Series
RFC 4444, *IS-IS MIB*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
RFC 4668, *RADIUS Accounting Client Management Information Base (MIB) for IPv6* (read-only access)	No exceptions	MX Series
RFC 4670, *RADIUS Accounting Client Management Information Base (MIB)* (read-only access)	No exceptions	MX Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 4801, *Definitions of Textual Conventions for Generalized Multiprotocol Label Switching (GMPLS) Management Information Base (MIB)* (read-only access)	No exceptions	M Series, MX Series, and T Series
RFC 4802, *Generalized Multiprotocol Label Switching (GMPLS) Traffic Engineering (TE) Management Information Base (MIB)* (read-only access)	Unsupported tables and objects: • **gmplsTunnelReversePerfTable** • **gmplsTeScalars** • **gmplsTunnelTable** • **gmplsTunnelARHopTable** • **gmplsTunnelCHopTable** • **gmplsTunnelErrorTable**	M Series, MX Series, and T Series
RFC 4803, *Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base (MIB)* (read-only access) **NOTE:** The tables in GMPLS TE (RFC 4802) and LSR (RFC 4803) MIBs are extensions of the corresponding tables from the MPLS TE (RFC 3812) and LSR (RFC 3813) MIBs and use the same index as the MPLS MIB tables.	Unsupported tables and objects: • **gmplsLabelTable** • **gmplsOutsegmentTable**	M Series, MX Series, and T Series
RFC 5132, *IP Multicast MIB* **NOTE:** This RFC obsoletes RFC2932.	Unsupported table: • **ipMcastZoneTable**	All platforms

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 5643, *Management Information Base for OSPFv3* (read-only access)	Unsupported tables and objects: • **ospfv3HostTable** • **ospfv3CfgNbrTable** • **ospfv3ExitOverflowInterval** • **ospfv3ReferenceBandwidth** • **ospfv3RestartSupport** • **ospfv3RestartInterval** • **ospfv3RestartStrictLsaChecking** • **ospfv3RestartStatus** • **ospfv3RestartAge** • **ospfv3RestartExitReason** • **ospfv3NotificationEnable** • **ospfv3StubRouterSupport** • **ospfv3StubRouterAdvertisement** • **ospfv3DiscontinuityTime** • **ospfv3RestartTime** • **ospfv3AreaNssaTranslatorRole** • **ospfv3AreaNssaTranslatorState** • **ospfv3AreaNssaTranslatorStabInterval** • **ospfv3AreaNssaTranslatorEvents** • **ospfv3AreaTEEnabled** • **ospfv3IfMetricValue** • **ospfv3IfDemandNbrProbe**	M Series, MX Series, PTX Series, SRX Series, and T Series

RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*	• Row creation
	• The **Set** operation
	• Unsupported tables and objects:
	  ◦ **vrrpv3StatisticsRowDiscontinuityTime**
	  ◦ **vrrpv3StatisticsPacketLengthErrors**
		ACX Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
RFC 7420, *Path Computation Element Communication*		MX Series and PTX Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
	The PCEP MIB module is limited to "read-only" access except for pcePcepNotificationsMaxRate, which is used to throttle the rate at which the implementation generates notifications. In the mentioned tables only PCEP peer and PCEP session table will be supported in this release. For **pcePcepPeerTable**, the following members are not supported: • **pcePcepPeerDiscontinuityTime TimeStamp,** • **pcePcepPeerLWMRspTime Unsigned32,** • **pcePcepPeerHWMRspTime Unsigned32,** • **pcePcepPeerNumPCReqSent Counter32,** • **pcePcepPeerNumPCReqRcvd Counter32,** • **pcePcepPeerNumPCRepSent Counter32,** • **pcePcepPeerNumPCRepRcvd Counter32,** • **pcePcepPeerAvgRspTime Unsigned32,** • **pcePcepPeerNumReqSent Counter32,** • **pcePcepPeerNumReqSentEroRcvd Counter32,** • **pcePcepPeerNumReqSentErrorRcvd Counter32,** • **pcePcepPeerNumReqSentTimeout Counter32,** • **pcePcepPeerNumReqSentPendRep Counter32,** • **pcePcepPeerNumReqSentCancelSent Counter32,** • **pcePcepPeerNumReqSentClosed Counter32,** • **pcePcepPeerNumReqRcvd Counter32,** • **pcePcepPeerNumPCNtfSent Counter32,** • **pcePcepPeerNumPCNtfRcvd Counter32,** • **pcePcepPeerNumSvecSent Counter32,** • **pcePcepPeerNumSvecReqSent Counter32,** • **pcePcepPeerNumSvecRcvd Counter32,** • **pcePcepPeerNumSvecReqRcvd Counter32,** • **pcePcepPeerNumReqRcvdPendRep Counter32,** • **pcePcepPeerNumReqRcvdEroSent Counter32,** • **pcePcepPeerNumReqRcvdNoPathSent Counter32,** • **pcePcepPeerNumReqRcvdCancelSent Counter32,** • **pcePcepPeerNumReqRcvdErrorSent Counter32,** • **pcePcepPeerNumReqRcvdCancelRcvd Counter32,**	

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
	• **pcePcepPeerNumReqRcvdClosed Counter32,** • **pcePcepPeerNumRepRcvdUnknown Counter32,** • **pcePcepPeerNumReqRcvdUnknown Counter32,** • **pcePcepPeerNumReqSentNoPathRcvd Counter32,** • **pcePcepPeerNumReqSentCancelRcvd Counter32**	

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
	For **pcePcepSessTable**, the following members are not supported: • **pcePcepSessNumPCReqSent Counter32,** • **pcePcepSessNumPCReqRcvd Counter32,** • **pcePcepSessKAHoldTimeRem Unsigned32,** • **pcePcepSessOverloaded TruthValue,** • **pcePcepSessOverloadTime Unsigned32,** • **pcePcepSessPeerOverloaded TruthValue,** • **pcePcepSessPeerOverloadTime Unsigned32,** • **pcePcepSessNumPCNtfSent Counter32,** • **pcePcepSessNumPCNtfRcvd Counter32,** • **pcePcepSessNumReqSent Counter32,** • **pcePcepSessNumReqSentPendRep Counter32,** • **pcePcepSessNumReqSentEroRcvd Counter32,** • **pcePcepSessNumReqSentNoPathRcvd Counter32,** • **pcePcepSessNumReqSentCancelRcvd Counter32,** • **pcePcepSessNumReqSentErrorRcvd Counter32,** • **pcePcepSessNumReqSentTimeout Counter32,** • **pcePcepSessNumReqSentCancelSent Counter32,** • **pcePcepSessAvgRspTime Unsigned32,** • **pcePcepSessLWMRspTime Unsigned32,** • **pcePcepSessHWMRspTime Unsigned32,** • **pcePcepSessNumSvecSent Counter32,** • **pcePcepSessNumSvecReqSent Counter32,** • **pcePcepSessNumReqRcvd Counter32,** • **pcePcepSessNumSvecRcvd Counter32,** • **pcePcepSessNumSvecReqRcvd Counter32,** • **pcePcepSessNumReqRcvdPendRep Counter32,** • **pcePcepSessNumReqRcvdEroSent Counter32,** • **pcePcepSessNumReqRcvdNoPathSent Counter32,** • **pcePcepSessNumReqRcvdCancelSent Counter32,** • **pcePcepSessNumReqRcvdErrorSent Counter32,** • **pcePcepSessNumReqRcvdCancelRcvd Counter32,** • **pcePcepSessNumRepRcvdUnknown Counter32,**	

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
	• **pcePcepSessNumReqRcvdUnknown Counter32**	
ESO Consortium MIB, which can be found at http://www.snmp.com/eso/ **NOTE:** The ESO Consortium MIB has been replaced by RFC 3826.	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
Internet Assigned Numbers Authority, *IANAiftype Textual Convention MIB*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
Internet draft draft-ietf-atommib-sonetaps-mib-10.txt, *Definitions of Managed Objects for SONET Linear APS Architectures*	As defined under the Juniper Networks enterprise branch [**jnxExperiment**] only	M Series, MX Series, and T Series
Internet draft draft-ieft-bfd-mib-02.txt, *Bidirectional Forwarding Detection Management Information Base*	(Represented by **mib-jnx-bfd-exp.txt** and implemented under the Juniper Networks enterprise branch [**jnxExperiment**]. Read only. Includes **bfdSessUp** and **bfdSessDown** traps. Does not support **bfdSessPerfTable** and **bfdSessMapTable**.)	ACX Series, EX Series, M Series, MX Series, SRX Series, and T Series
Internet draft draft-ietf-idmr-igmp-mib-13.txt, *Internet Group Management Protocol (IGMP) MIB*	No exceptions	EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
Internet draft draft-ietf-idmr-pim-mib-09.txt, *Protocol Independent Multicast (PIM) MIB*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series , and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
Internet draft draft-ietf-isis-wg-mib-07.txt, *Management Information Base for IS-IS* **NOTE:** Replaced with RFC 4444, *IS-IS MIB* in Junos OS Release 11.3 and later.	Unsupported tables and objects: • **isisISAdjTable** • **isisISAdjAreaAddrTable** • **isisISAdjIPAddrTable** • **isisISAdjProtSuppTable)**	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series
Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*	(Implemented under the Juniper Networks enterprise branch [**jnxExperiment**]. OID for **jnxMvpnExperiment** is **.1.3.6.1.4.1.2636.5.12**. Read only. Includes **jnxMvpnNotifications** traps.)	M Series, MX Series, and T Series
Internet draft draft-ietf-mpls-mldp-mib-02.txt, *Definitions of Managed Objects for the LDP Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*	No exceptions	M Series, MX Series, PTX Series, and T Series
Internet draft draft-ietf-mpls-p2mp-te-mib-09.txt, *P2MP MPLS-TE MIB* (read-only access)	Unsupported table: • **mplsTeP2mpTunnelBranchPerfTable**	ACX Series, M Series, MX Series, PTX Series, and T Series
Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, *Management Information Base for OSPFv3*	Support for **ospfv3NbrTable** only.	M Series, MX Series, PTX Series, SRX Series, and T Series
Internet draft draft-ietf-ppvpn-mpls-vpn-mib-04.txt, *MPLS/BGP Virtual Private Network Management Information Base Using SMIv2*	Supported tables and objects: • **mplsVpnScalars** • **mplsVpnVrfTable** • **mplsVpnPerTable** • **mplsVpnVrfRouteTargetTable**	M Series, MX Series, PTX Series, and T Series

Table 30: Standard MIBs supported by Junos OS *(continued)*

Standard MIB	Exceptions	Platforms
Internet draft draft-kamarthy-gdoi-mib-01, *Management Information Base for the Group Domain of Interpretation (GDOI)*	Caveats: • The GDOI MIB from the IETF draft is modified to include only the group member tables and notifications. • Only the SNMP notifications that are applicable to MX Series group members are supported.	MX Series
Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*	No exceptions	ACX Series, EX Series, M Series, MX Series, PTX Series, SRX Series, and T Series

For information about standard SNMP MIB objects, see the SNMP MIB Explorer.

RELATED DOCUMENTATION

Enterprise-Specific SNMP MIBs Supported by Junos OS | 436

Enterprise-Specific MIBs for Junos OS Evolved on PTX10003 Devices

Starting in Junos OS Evolved Release 19.1R1, the enterprise-specific MIBs listed in Table 29 on page 436 are supported. For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer.

Table 31: Enterprise-Specific MIBs Supported by Junos OS Evolved

Enterprise-Specific MIB	Description	Exceptions
BGP4 V2 MIB	Provides support for monitoring BGP peer-received prefix counters. It is based upon similar objects in the MIB documented in Internet draft draft-ietf-idr-bgp4-mibv2-03.txt, *Definitions of Managed Objects for the Fourth Version of BGP (BGP-4), Second Version*.	No exceptions

Table 31: Enterprise-Specific MIBs Supported by Junos OS Evolved *(continued)*

Enterprise-Specific MIB	Description	Exceptions
Chassis MIBs	Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and air flow) and inventory support for the chassis, System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), Switch Fabric Board (SFB), Flexible PIC Concentrators (FPCs), and PICs.	Supported traps: • jnxFruInsertion • jnxFruRemoval • jnxFruPowerOn • jnxFruPowerOff • jnxFruOnline • jnxFruOffline • jnxFruFailed • jnxFruOK • jnxPowerSupplyFailure • jnxPowerSupplyOK • jnxPowerSupplyInputFailure • jnxPowerSupplyInputOK • jnxFanFailure • jnxFanOK • jnxOverTemperature • jnxTemperatureOK Supported tables and objects: • jnxBoxClass • jnxBoxDescr • jnxBoxSerialNo • jnxBoxRevision • jnxBoxInstalled • jnxContentsLastChange • jnxContainersTable • jnxOperatingTable • jnxRedundancyTable • jnxContentsTable • jnxFilledTable • jnxFruTable
Class-of-Service MIB	Provides support for monitoring interface output queue statistics per interface and per forwarding class.	No exceptions

Table 31: Enterprise-Specific MIBs Supported by Junos OS Evolved *(continued)*

Enterprise-Specific MIB	Description	Exceptions
Host Resources MIB	Extends the hrStorageTable object, providing a measure of the usage of each file system on the router in percentage format. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.	Supported tables and objects: • hrStorageTable • jnxHrStorage • hrSWInstalledTable • hrSystemUptime • hrSystemDate • hrSystemInitialLoadDevice • hrSystemInitialLoadParameters • hrSystemNumUsers • hrSystemProcesses • hrSystemMaxProcesses • hrMemorySize • hrSWInstalledLastChange • hrSWInstalledLastUpdateTime
Interface MIB	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information.	No exceptions
IPv4 MIB	Provides additional IPv4 address information, supporting the assignment of identical IPv4 addresses to separate interfaces.	No exceptions
IPv6 and ICMPv6 MIB	Provides IPv6 and Internet Control Message Protocol version 6 (ICMPv6) statistics.	Unsupported objects • jnxIcmpv6GlobalStats branch and the objects under it
LDP MIB	Provides LDP statistics and defines LDP label-switched path (LSP) notifications. LDP traps support only IPv4 standards.	No exceptions
MPLS LDP MIB	Contains object definitions as described in RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*.	No exceptions

Table 31: Enterprise-Specific MIBs Supported by Junos OS Evolved *(continued)*

Enterprise-Specific MIB	Description	Exceptions
MPLS MIB	Provides MPLS information and defines MPLS notifications.	No exceptions
RSVP MIB	Provides information about RSVP-traffic engineering sessions that correspond to MPLS LSPs on transit routers in the service provider core network.	No exceptions
SFF Digital Optical Monitor MIB	Defines objects used for Digital Optical Monitor on interfaces of Juniper products.	Supported tables: • jnxDomCurrentTable • jnxDomModuleLaneTable
VPN MIB	Provides monitoring for Layer 3 VPNs, Layer 2 VPNs, and virtual private LAN service (VPLS).	Unsupported objects • jnxVpnActiveVpns • jnxVpnConfiguredVpns

RELATED DOCUMENTATION

- Enterprise-Specific SNMP MIBs Supported by Junos OS | **436**
- Standard SNMP MIBs Supported by Junos OS | **452**
- Standard MIBs for Junos OS Evolved on PTX10003 Devices | **482**
- Configuring SNMP Traps | **583**

Standard MIBs for Junos OS Evolved on PTX10003 Devices

Starting in Junos OS Evolved Release 19.1R1, the Standard MIBs listed in Table 30 on page 452 are supported. For information about Standard MIB objects, see the SNMP MIB Explorer.

Table 32: Standard MIBs Supported by Junos OS Evolved

Standard MIB	Exceptions
RFC 1155, *Structure and Identification of Management Information for TCP/IP-Based Internets*	No exceptions

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
RFC 1157, *A Simple Network Management Protocol (SNMP)*	No exceptions
RFC 1212, *Concise MIB Definitions*	No exceptions
RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	Unsupported tables and objects: • ICMP group
RFC 1215, *A Convention for Defining Traps for Use with the SNMP*	No exceptions
RFC 1850, *OSPF Version 2 Management Information Base*	No exceptions
RFC 1901, *Introduction to Community-Based SNMPv2*	No exceptions
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	No exceptions
RFC 2096, *IP Forwarding Table MIB*	No exceptions
RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*	Supported tables and objects: • ipv6AddrTable • ipv6NetToMediaTable • ipv6IfTable • ipv6IfStatsTable • ipv6AddrPrefixTable • ipv6IfTableLastChange • ipv6Interfaces • ipv6Forwarding • ipv6DefaultHopLimit
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	No exceptions
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	No exceptions
RFC 2579, *Textual Conventions for SMIv2*	No exceptions

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
RFC 2580, *Conformance Statements for SMIv2*	No exceptions
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*	Unsupported tables and objects: • dot3
RFC 2790, *Host Resources MIB*	Unsupported tables and objects: • hrDeviceTable • hrSWRunTable • hrSWRunPerfTable
RFC 2863, *The Interfaces Group MIB*	No exceptions
RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*	No exceptions
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	No exceptions
RFC 2932, *IPv4 Multicast Routing MIB*	No exceptions
RFC 2934, *Protocol Independent Multicast MIB for IPv4*	No exceptions
RFC 2981, *Event MIB*	No exceptions
RFC 3014, *Notification Log MIB*	No exceptions
RFC 3019, *IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol*	No exceptions
RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework*	No exceptions
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	No exceptions
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	No exceptions
RFC 3413, *Simple Network Management Protocol (SNMP) Applications*	No exceptions

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
RFC 3414, *User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*	No exceptions
RFC 3415, *View-Based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*	No exceptions
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	No exceptions
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	No exceptions
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	No exceptions
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	No exceptions
RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*	No exceptions
RFC 3811, *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*	No exceptions
RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)* (read-only access)	No exceptions
RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*	Unsupported tables and objects (read only access): • mplsInterfacePerfTable • mplsInSegmentPerfTable • mplsOutSegmentPerfTable • mplsInSegmentMapTable • mplsXCUp • mplsXCDown
RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-Based Security Model*	No exceptions

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
RFC 3877, *Alarm Management Information Base*	No exceptions
RFC 4133, Entity MIB	Supported table: • entPhysicalTable
RFC 4292, *IP Forwarding MIB*	No exceptions
RFC 4293, Management Information Base for the Internet Protocol (IP)	Supported tables: • ipAddressTable • ipAddrTable • ipNetToPhysicalTable • ipNetToMediaTable • ipSystemStatsTable Unsupported objects: • icmpMsgStatsIPVersion • icmpMsgStatsType • icmpMsgStatsInPkts • icmpMsgStatsOutPkts • icmpStatsIPVersion • icmpStatsInMsgs • icmpStatsInErrors • icmpStatsOutMsgs • icmpStatsOutErrors
RFC 4444, *IS-IS MIB*	No exceptions
RFC 5643, *Management Information Base for OSPFv3* (read-only access)	No exceptions

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
IEEE, 802.3ad, *Aggregation of Multiple Link Segments*	

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
	Supported objects for PTX10008 on Junos OS Evolved Release 20.1R1: • **dot3adAggPortStatsLACPDUsRx**, **dot3adAggPortStatsMarkerPDUsRx**, **dot3adAggPortStatsMarkerResponsePDUsRx**, **dot3adAggPortStatsUnknownRx**, **dot3adAggPortStatsIllegalRx**, **dot3adAggPortStatsLACPDUsTx**, **dot3adAggPortStatsMarkerPDUsTx**, and **dot3adAggPortStatsMarkerResponsePDUsTx** • **dot3adInterfaceName**, **dot3adOperState**, **dot3adAggname**, and **dot3adInterfaceTimeout**. Unsupported objects for PTX10008 on Junos OS Evolved Release 20.1R1: • **dot3adAggActorSystemPriority**, **dot3adAggActorSystemID**, **dot3adAggActorAdminKey**, and **dot3adAggActorOperKey**. • **dot3adAggMACAddress**, **dot3adAggAggregateOrIndividual**, **dot3adAggPartnerSystemID**, **dot3adAggPartnerSystemPriority**, **dot3adAggPartnerOperKey**, **dot3adAggCollectorMaxDelay**, **dot3adAggPortListPorts**, and **dot3adTablesLastChanged** • **dot3adAggPortActorSystemPriority**, **dot3adAggPortActorSystemID**, **dot3adAggPortActorAdminKey**, **dot3adAggPortActorOperKey**, **dot3adAggPortActorPort**,**dot3adAggPortActorPortPriority**, **dot3adAggPortActorAdminState**, and **dot3adAggPortActorOperState** • **dot3adAggPortPartnerAdminSystemPriority**, **dot3adAggPortPartnerOperSystemPriority**, **dot3adAggPortPartnerAdminSystemID**, **dot3adAggPortPartnerOperSystemID**, **dot3adAggPortPartnerAdminKey**,**dot3adAggPortPartnerOperKey**, **dot3adAggPortPartnerAdminPort**, **dot3adAggPortPartnerOperPort**, **dot3adAggPortPartnerAdminPortPriority**, and

Table 32: Standard MIBs Supported by Junos OS Evolved *(continued)*

Standard MIB	Exceptions
	dot3adAggPortPartnerOperPortPriority • **dot3adAggPortDebugRxState**, **dot3adAggPortDebugLastRxTime**, **dot3adAggPortDebugMuxState**, **dot3adAggPortDebugMuxReason**, **dot3adAggPortDebugActorChurnState**, **dot3adAggPortDebugPartnerChurnState**, **dot3adAggPortDebugActorChurnCount**, **dot3adAggPortDebugPartnerChurnCount**, **dot3adAggPortDebugActorSyncTransitionCount**, **dot3adAggPortDebugPartnerSyncTransitionCount**, **dot3adAggPortDebugActorChangeCount**, and **dot3adAggPortDebugPartnerChangeCount**.
Internet Assigned Numbers Authority, *IANAiftype Textual Convention MIB*	No exceptions
Internet draft draft-ietf-idmr-igmp-mib-13.txt, *Internet Group Management Protocol (IGMP) MIB*	No exceptions
Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*	No exceptions
Internet draft draft-ietf-isis-wg-mib-07.txt, *Management Information Base for IS-IS*	No exceptions
Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, *Management Information Base for OSPFv3*	No exceptions
Internet draft draft-ietf-idmr-pim-mib-09.txt, *Protocol Independent Multicast (PIM) MIB*	No exceptions
Internet Draft P2MP MPLS-TE MIB (draft-ietf-mpls-p2mp-te-mib-09.txt) (read-only access)	No exceptions

RELATED DOCUMENTATION

Enterprise-Specific SNMP MIBs Supported by Junos OS | 436

Enterprise-Specific MIBs for Junos OS Evolved on PTX10003 Devices | 479
Standard SNMP MIBs Supported by Junos OS | 452
Configuring SNMP Traps | 583

Standard SNMP Traps Supported by Junos OS

This topic provides the list of standard SNMPv1 and SNMPv2 traps supported by devices running Junos OS. For more information about traps see SNMP MIB Explorer.

Starting in Junos OS Release 20.1, after graceful routing engine switchover (GRES), the new master Routing Engine sends a single warmStart notification. The master Routing Engine sends a **coldStart** notification when the device comes up. The master Routing Engine also sends **warmStart** notifications for subsequent restarts of the SNMP daemon. After GRES, the new master Routing Engine sends a single **warmStart** notification and the backup Routing Engine does not send any notification.

Standard SNMP Version 1 Traps

Table 33 on page 490 provides an overview of the standard traps for SNMPv1. The traps are organized first by trap category and then by trap name, and include their enterprise ID, generic trap number, and specific trap number. The system logging severity levels are listed for those traps that have them with their corresponding system log tag. Traps that do not have corresponding system logging severity levels are marked with an en dash (–) in the table.

For more information about system log messages, see the System Log Explorer.

Table 33: Standard Supported SNMP Version 1 Traps

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
Startup Notifications							
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	**authenticationFailure**	1.3.6.1.4.1.2636	4	0	Notice	SNMPD_ TRAP_ GEN_FAILURE	All devices running Junos OS.
	coldStart	1.3.6.1.4.1.2636	0	0	Critical	SNMPD_TRAP_ COLD_START	All devices running Junos OS.
	warmStart	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_ WARM_START	All devices running Junos OS.

Table 33: Standard Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
Link Notifications							
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	**linkDown**	1.3.6.1.4.1.2636	2	0	Warning	SNMP_ TRAP_ LINK_DOWN	All devices running Junos OS.
	linkUp	1.3.6.1.4.1.2636	3	0	Info	SNMP_TRAP_ LINK_UP	All devices running Junos OS.
Remote Operations Notifications							
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	**pingProbeFailed**	1.3.6.1.2.1.80.0	6	1	Info	SNMP_TRAP _PING_ PROBE_ FAILED	All devices running Junos OS.
	pingTestFailed	1.3.6.1.2.1.80.0	6	2	Info	SNMP_TRAP_ PING_TEST _FAILED	All devices running Junos OS.
	pingTestCompleted	1.3.6.1.2.1.80.0	6	3	Info	SNMP_TRAP_ PING_TEST_ COMPLETED	All devices running Junos OS.
	traceRoutePathChange	1.3.6.1.2.1.81.0	6	1	Info	SNMP_TRAP_ TRACE_ROUTE_ PATH_CHANGE	All devices running Junos OS.
	traceRouteTestFailed	1.3.6.1.2.1.81.0	6	2	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_FAILED	All devices running Junos OS.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0	6	3	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_COMPLETED	All devices running Junos OS.
RMON Alarms							

Table 33: Standard Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
RFC 2819a, *RMON MIB*	**fallingAlarm**	1.3.6.1.2.1.16	6	2	–	–	All devices running Junos OS.
	risingAlarm	1.3.6.1.2.1.16	6	1	–	–	All devices running Junos OS.
Routing Notifications							
BGP 4 MIB	**bgpEstablished**	1.3.6.1.2.1.15.7	6	1	–	–	M, T, MX, J, EX, and SRX Series devices.
	bgpBackwardTransition	1.3.6.1.2.1.15.7	6	2	–	–	M, T, MX, J, EX, and SRX Series devices.

Table 33: Standard Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
OSPF TRAP MIB	**ospfVirtIfStateChange**	1.3.6.1.2.1.14.16.2	6	1	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2	6	2	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2	6	3	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfIfConfigError	1.3.6.1.2.1.14.16.2	6	4	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2	6	5	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2	6	6	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2	6	7	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	8	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	9	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2	6	10	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2	6	11	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2	6	13	–	–	M, T, MX, J, EX, and SRX Series devices.
	ospfIfStateChange	1.3.6.1.2.1.14.16.2	6	16	–	–	M, T, MX, J, EX, and SRX Series devices.

Table 33: Standard Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
VRRP Notifications							
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	**vrrpTrapNewMaster**	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW MASTER_TRAP	All devices running Junos OS.
	vrrpTrapAuthFailure	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_ FAILURE_TRAP	All devices running Junos OS.
RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*	**vrrpv3NewMaster**	1.3.6.1.2.1.207	6	1	Warning	VRRPD_NEW_MASTER	M and MX
	vrrpv3ProtoError	1.3.6.1.2.1.207	6	2	Warning	VRRPD_V3_PROTO_ERROR	M and MX

Standard SNMP Version 2 Traps

Table 34 on page 495 provides an overview of the standard SNMPv2 traps supported by the Junos OS. The traps are organized first by trap category and then by trap name and include their **snmpTrapOID**. The system logging severity levels are listed for those traps that have them with their corresponding system log tag. Traps that do not have corresponding system logging severity levels are marked with an en dash (–) in the table.

Table 34: Standard Supported SNMP Version 2 Traps

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
Startup Notifications					
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	**coldStart**	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_COLD_START	All devices running Junos OS.
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START	All devices running Junos OS.
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_GEN_FAILURE	All devices running Junos OS.
Link Notifications					
RFC 2863, *The Interfaces Group MIB*	**linkDown**	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_LINK_DOWN	All devices running Junos OS.
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_LINK_UP	All devices running Junos OS.
Remote Operations Notifications					

Table 34: Standard Supported SNMP Version 2 Traps *(continued)*

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	**pingProbeFailed**	1.3.6.1.2.1.80.0.1	Info	SNMP_TRAP_PING_PROBE_FAILED	All devices running Junos OS.
	pingTestFailed	1.3.6.1.2.1.80.0.2	Info	SNMP_TRAP_PING_TEST_FAILED	All devices running Junos OS.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Info	SNMP_TRAP_PING_TEST_COMPLETED	All devices running Junos OS.
	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE	All devices running Junos OS.
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED	All devices running Junos OS.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED	All devices running Junos OS.
RMON Alarms					
RFC 2819a, *RMON MIB*	**fallingAlarm**	1.3.6.1.2.1.16.0.1	–	–	All devices running Junos OS.
	risingAlarm	1.3.6.1.2.1.16.0.2	–	–	All devices running Junos OS.
Routing Notifications					
BGP 4 MIB	**bgpEstablished**	1.3.6.1.2.1.15.7.1	–	–	All devices running Junos OS.
	bgpBackwardTransition	1.3.6.1.2.1.15.7.2	–	–	All devices running Junos OS.

Table 34: Standard Supported SNMP Version 2 Traps *(continued)*

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
OSPF Trap MIB	**ospfVirtIfStateChange**	1.3.6.1.2.1.14.16.2.1	–	–	All devices running Junos OS.
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	–	–	All devices running Junos OS.
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	–	–	All devices running Junos OS.
	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	–	–	All devices running Junos OS.
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	–	–	All devices running Junos OS.
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	–	–	All devices running Junos OS.
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	–	–	All devices running Junos OS.
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	–	–	All devices running Junos OS.
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	–	–	All devices running Junos OS.
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	–	–	All devices running Junos OS.
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	–	–	All devices running Junos OS.
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	–	–	All devices running Junos OS.
	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	–	–	All devices running Junos OS.

Table 34: Standard Supported SNMP Version 2 Traps *(continued)*

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
MPLS Notifications					
RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base*	**mplsTunnelUp**				
	mplsTunnelDown				
	mplsTunnelRerouted				
	mplsTunnelReoptimized				
Entity State MIB Notifications					
RFC 4268, *Entity State MIB*	**entStateOperEnabled**	1.3.6.1.2.1.131.0.1	Notice	CHASSISD_SNMP_TRAP3	MX240, MX480, and MX960
	entStateOperDisabled	1.3.6.1.2.1.131.0.2	Notice	CHASSISD_SNMP_TRAP3	MX240, MX480, and MX960
L3VPN Notifications					
RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN)*	**mplsL3VpnVrfUp**				
	mplsL3VpnVrfDown				
	mplsL3VpnVrf RouteMidThresh Exceeded				
	mplsL3VpnVrf NumVrfRouteMax ThreshExceeded				
	mplsL3VpnNum VrfRouteMax ThreshCleared				
VRRP Notifications					

Table 34: Standard Supported SNMP Version 2 Traps *(continued)*

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	**vrrpTrapNewMaster**	1.3.6.1.2.1.68.0.1	Warning	VRRPD_ NEWMASTER_ TRAP	All devices running Junos OS.
	vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	Warning	VRRPD_AUTH_ FAILURE_ TRAP	All devices running Junos OS.
RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*	**vrrpv3NewMaster**	1.3.6.1.2.1.207.0.1	Warning	VRRPD_NEW_MASTER	M and MX
	vrrpv3ProtoError	1.3.6.1.2.1.207.0.2	Warning	VRRPD_V3_PROTO_ERROR	M and MX

Release History Table

Release	Description
20.1R1	Starting in Junos OS Release 20.1, after graceful routing engine switchover (GRES), the new master Routing Engine sends a single warmStart notification.

RELATED DOCUMENTATION

- Enterprise-Specific SNMP Traps Supported by Junos OS | **500**
- Enterprise-Specific SNMP MIBs Supported by Junos OS | **436**
- Standard SNMP MIBs Supported by Junos OS | **452**
- Configuring SNMP Trap Options and Groups on a Device Running Junos OS | **585**
- Managing Traps and Informs | **432**

Enterprise-Specific SNMP Traps Supported by Junos OS

IN THIS SECTION

- Juniper Networks Enterprise-Specific SNMP Version 1 Traps | 500
- Juniper Networks Enterprise-Specific SNMP Version 2 Traps | 510

This topic provides the list of Juniper Networks enterprise-specific SNMPv1and SNMPv2 traps supported on devices running Junos OS. For more information about traps see SNMP MIB Explorer.

Juniper Networks Enterprise-Specific SNMP Version 1 Traps

The Junos OS supports enterprise-specific SNMP version 1 traps shown in Table 35 on page 500. The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
Chassis Notifications (Alarm Conditions)							
Chassis MIB (**jnx-chassis.mib**)	**jnxPowerSupplyFailure**	1.3.6.1.4.1.2636.4.1	6	1	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFanFailure	1.3.6.1.4.1.2636.4.1	6	2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1	6	3	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
	jnxRedundancySwitchOver	1.3.6.1.4.1.2636.4.1	6	4	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1	6	7	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1	6	8	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruFailed	1.3.6.1.4.1.2636.4.1	6	9	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruOffline	1.3.6.1.4.1.2636.4.1	6	10	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruOnline	1.3.6.1.4.1.2636.4.1	6	11	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruCheck	1.3.6.1.4.1.2636.4.1	6	12	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
	jnxFEBSwitchover	1.3.6.1.4.1.2636.4.1	6	13	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxHardDiskFailed	1.3.6.1.4.1.2636.4.1	6	14	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxHardDiskMissing	1.3.6.1.4.1.2636.4.1	6	15	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxPowerSupplyOk	1.3.6.1.4.1.2636.4.2	6	1	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFanOK	1.3.6.1.4.1.2636.4.2	6	2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2	6	3	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.
Configuration Notifications							
Configuration Management MIB (**jnx-configmgmt.mib**)	**jnxCmCfgChange**	1.3.6.1.4.1.2636.4.5	6	1	–	–	All devices running Junos OS.
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5	6	2	–	–	All devices running Junos OS.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
Link Notifications							

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
Flow Collection Services MIB (**jnx-coll.mib**)	**jnxCollUnavailableDest**	1.3.6.1.4.1.2636.4.8	6	1	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollUnavailableDestCleared	1.3.6.1.4.1.2636.4.8	6	2	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollUnsuccessfulTransfer	1.3.6.1.4.1.2636.4.8	6	3	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollFlowOverload	1.3.6.1.4.1.2636.4.8	6	4	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollFlowOverloadCleared	1.3.6.1.4.1.2636.4.8	6	5	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollMemoryUnavailable	1.3.6.1.4.1.2636.4.8	6	6	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollMemoryAvailable	1.3.6.1.4.1.2636.4.8	6	7	–	–	

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
							Devices that run Junos OS and have collector PICs installed.
	jnxCollFtpSwitchover	1.3.6.1.4.1.2636.4.8	6	8	–	–	Devices that run Junos OS and have collector PICs installed.
Passive Monitoring MIB **(jnx-pmon.mib)**	**jnxPMonOverloadSet**	1.3.6.1.4.1.2636.4.7.0.1	6	1	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
	jnxPMonOverloadCleared	1.3.6.1.4.1.2636.4.7.0.2	6	2	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
SONET APS MIB (**jnx-sonetaps.mib**)	**apsEventChannelMismatch**	1.3.6.1.4.1.2636.3.24.2	6	3	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventPSBF	1.3.6.1.4.1.2636.3.24.2	6	4	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventFEPLF	1.3.6.1.4.1.2636.3.24.2	6	5	–	–	Devices that run Junos OS and have SONET PICs installed.
Remote Operations							
PING MIB (**jnx-ping.mib**)	**jnxPingRttThresholdExceeded**	1.3.6.1.4.1.2636.4.9	6	1	–	–	All devices running Junos OS.
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	2	–	–	All devices running Junos OS.
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	3	–	–	All devices running Junos OS.
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	4	–	–	All devices running Junos OS.
	jnxPingEgressStdDev ThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	5	–	–	All devices running Junos OS.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
	jnxPingEgressJitterThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	6	–	–	All devices running Junos OS.
	jnxPingIngressThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	7	–	–	All devices running Junos OS.
	jnxPingIngressStddevThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	8	–	–	All devices running Junos OS.
	jnxPingIngressJitterThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	9	–	–	All devices running Junos OS.
Routing Notifications							
BFD Experimental MIB (**jnx-bfd-exp.mib**)	**bfdSessUp**	1.3.6.1.4.1.2636.5.3.1	6	1	–	–	All devices running Junos OS.
	bfdSessDown	1.3.6.1.4.1.2636.5.3.1	6	2	–	–	All devices running Junos OS.

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
LDP MIB (**jnx-ldp.mib**)	**jnxLdpLspUp**	1.3.6.1.4.1.2636.4.4	6	1	–	–	M, T, and MX Series routers.
	jnxLdpLspDown	1.3.6.1.4.1.2636.4.4	6	2	–	–	M, T, and MX Series routers.
	jnxLdpSesUp	1.3.6.1.4.1.2636.4.4	6	3	–	–	M, T, and MX Series routers.
	jnxLdpSesDown	1.3.6.1.4.1.2636.4.4	6	4	–	–	M, T, and MX Series routers.
MPLS MIB (**jnx-mpls.mib**)	**mplsLspUp** (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	1	–	–	
	mplsLspDown (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	2	–	–	
	mplsLspChange (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	3	–	–	
	mplsLspPathDown (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	4	–	–	

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
VPN MIB (**jnx-vpn.mib**)	**jnxVpnIfUp**	1.3.6.1.4.1.2636.3.26	6	1	–	–	M, T, and MX Series routers.
	jnxVpnIfDown	1.3.6.1.4.1.2636.3.26	6	2	–	–	M, T, and MX Series routers.
	jnxVpnPwUp	1.3.6.1.4.1.2636.3.26	6	3	–	–	M, T, and MX Series routers.
	jnxVpnPwDown	1.3.6.1.4.1.2636.3.26	6	4	–	–	M, T, and MX Series routers.
RMON Alarms							
RMON MIB (**jnx-rmon.mib**)	**jnxRmonAlarmGetFailure**	1.3.6.1.4.1.2636.4.3	6	1	–	–	All devices running Junos OS.
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3	6	2	–	–	All devices running Junos OS.
SONET Alarms							

Table 35: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
SONET MIB (**jnx-sonet.mib**)	**jnxSonetAlarmSet**	1.3.6.1.4.1.2636.4.6	6	1	–	–	Devices that run Junos OS and have SONET PICs installed.
	jnxSonetAlarmCleared	1.3.6.1.4.1.2636.4.6	6	2	–	–	Devices that run Junos OS and have SONET PICs installed.
Timing Alarms							
Timing MIB	**jnxTimingAlarmLossOfReference1**	1.3.6.1.4.1.2636.3.75.1.1	6	35	Critical	–	ACX710
	jnxTimingAlarmLossOfReference2	1.3.6.1.4.1.2636.3.75.1.1	6	37	Critical	–	ACX710
	jnxTimingAlarmQlBelowThreshold	1.3.6.1.4.1.2636.3.75.1.1	6	45	Critical	-	ACX710
	jnxTimingAlarmNoMoreReference	1.3.6.1.4.1.2636.3.75.1.1	6	43	Critical	-	ACX710
	jnxTimingAlarmTodInSignalFail	1.3.6.1.4.1.2636.3.75.1.1	6	49	Critical	-	ACX710
	jnxTimingAlarmPtpLocalClockOutOfSync	1.3.6.1.4.1.2636.3.75.1.1	6	33	Critical	-	ACX710
	jnxTimingAlarmNoForeignMaster	1.3.6.1.4.1.2636.3.75.1.1	6	29	Critical	-	ACX710

Juniper Networks Enterprise-Specific SNMP Version 2 Traps

The Junos OS supports the enterprise-specific SNMP version 2 traps shown in Table 36 on page 511. The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

For more information about system messages, see the System Log Explorer. For more information about configuring system logging, see the Junos OS Administration Library for Routing Devices.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
Chassis (Alarm Conditions) Notifications					
Chassis MIB (**jnx-chassis.mib**)	**jnxPowerSupplyFailure**	1.3.6.1.4.1.2636.4.1.1	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFanFailure	1.3.6.1.4.1.2636.4.1.2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1.3	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruNotifAdminStatus		Notice		
	jnxFruNotifMismatch		Notice		
	jnxFruNotifOperStatus		Notice		
	jnxRedundancySwitchOver	1.3.6.1.4.1.2636.4.1.4	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1.5	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1.6	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1.7	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1.8	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruFailed	1.3.6.1.4.1.2636.4.1.9	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruOffline	1.3.6.1.4.1.2636.4.1.10	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
	jnxFruOnline	1.3.6.1.4.1.2636.4.1.11	Notice	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.
	jnxFruCheck	1.3.6.1.4.1.2636.4.1.12	Notice	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.
	jnxFEBSwitchover	1.3.6.1.4.1.2636.4.1.13	Notice	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.
	jnxHardDiskFailed	1.3.6.1.4.1.2636.4.1.14	Notice	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.
	jnxHardDiskMissing	1.3.6.1.4.1.2636.4.1.15	Notice	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.
jnxPowerSupplyOK	1.3.6.1.4.1.2636.4.2.1	Critical	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.	
jnxFanOK	1.3.6.1.4.1.2636.4.2.2	Critical	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.	
jnxTemperatureOK	1.3.6.1.4.1.2636.4.2.3	Alert	CHASSISD_ SNMP_ TRAP	All devices running Junos OS.	
Configuration Notifications					
Configuration Management MIB (**jnx-cfgmgmt.mib**)	**jnxCmCfgChange**	1.3.6.1.4.1.2636.4.5.0.1	–	–	All devices running Junos OS.
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–	All devices running Junos OS.
Link Notifications					

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
Flow Collection Services MIB (**jnx-coll.mib**)	**jnxCollUnavailableDest**	1.3.6.1.4.1.2636.4.8.0.1	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollUnavailableDestCleared	1.3.6.1.4.1.2636.4.8.0.2	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollUnsuccessfulTransfer	1.3.6.1.4.1.2636.4.8.0.3	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollFlowOverload	1.3.6.1.4.1.2636.4.8.0.4	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollFlowOverloadCleared	1.3.6.1.4.1.2636.4.8.0.5	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollMemoryUnavailable	1.3.6.1.4.1.2636.4.8.0.6	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollMemoryAvailable	1.3.6.1.4.1.2636.4.8.0.7	–	–	Devices that run Junos OS and have collector PICs installed.
	jnxCollFtpSwitchover	1.3.6.1.4.1.2636.4.8.0.8	–	–	Devices that run Junos OS and have collector PICs installed.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
PMON MIB (**jnx-pmon.mib**)	**jnxPMonOverloadSet**	1.3.6.1.4.1.2636.4.7.0.1	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
	jnxPMonOverloadCleared	1.3.6.1.4.1.2636.4.7.0.2	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
SONET APS MIB (**jnx-sonetaps.mib**)	**apsEventChannelMismatch**	1.3.6.1.4.1.2636.3.24.2.0.3	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventPSBF	1.3.6.1.4.1.2636.3.24.2.0.4	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventFEPLF	1.3.6.1.4.1.2636.3.24.2.0.5	–	–	Devices that run Junos OS and have SONET PICs installed.
Remote Operations Notifications					

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
PING MIB (**jnx-ping.mib**)	**jnxPingRttThreshold Exceeded**	1.3.6.1.4.1.2636.4.9.0.1	–	–	All devices running Junos OS.
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–	All devices running Junos OS.
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–	All devices running Junos OS.
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–	All devices running Junos OS.
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–	All devices running Junos OS.
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–	All devices running Junos OS.
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–	All devices running Junos OS.
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–	All devices running Junos OS.
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–	All devices running Junos OS.
Routing Notifications					
BFD Experimental MIB (**jnx-bfd-exp.mib**)	**bfdSessUp**	1.3.6.1.4.1.2636.5.3.1.0.1	–	–	All devices running Junos OS.
	bfdSessDown	1.3.6.1.4.1.2636.5.3.1.0.2	–	–	All devices running Junos OS.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
BGP4 V2 MIB (**jnx-bgpmib2.mib**)	**jnxBgpM2Established**	1.3.6.1.4.1.2636.5.1.1.10.1	–	–	All devices running Junos OS.
	jnxBgpM2BackwardTransition	1.3.6.1.4.1.2636.5.1.1.10.2	–	–	All devices running Junos OS.
DHCP MIB (**jnx-dhcp.mib**)	**jnxJdhcpLocalServer DuplicateClient**	1.3.6.1.4.1.2636.3.61.1.3.1	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer InterfaceLimitExceeded	1.3.6.1.4.1.2636.3.61.1.3.2	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer InterfaceLimitAbated	1.3.6.1.4.1.2636.3.61.1.3.3	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer Health	1.3.6.1.4.1.2636.3.61.1.3.4	–	–	All devices running Junos OS.
	jnxJdhcpRelayInterface LimitExceeded	1.3.6.1.4.1.2636.3.61.2.3.1	–	–	All devices running Junos OS.
	jnxJdhcpRelayInterface LimitAbated	1.3.6.1.4.1.2636.3.61.2.3.2	–	–	All devices running Junos OS.
DHCPv6MIB (**jnx-dhcpv6.mib**)	**jnxJdhcpv6LocalServer InterfaceLimitExceeded**	1.3.6.1.4.1.2636.3.62.6.2.3.1	–	–	All devices running Junos OS.
	jnxJdhcpv6LocalServer InterfaceLimitAbated	1.3.6.1.4.1.2636.3.62.6.2.3.2	–	–	All devices running Junos OS.
	jnxJdhcpv6LocalServer Health	1.3.6.1.4.1.2636.3.62.6.2.3.3	–	–	All devices running Junos OS.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
LDP MIB (**jnx-ldp.mib**)	**jnxLdpLspUp**	1.3.6.1.4.1.2636.4.4.0.1	–	–	M, T, and MX Series routers.
	jnxLdpLspDown	1.3.6.1.4.1.2636.4.4.0.2	–	–	M, T, and MX Series routers.
	jnxLdpSesUp	1.3.6.1.4.1.2636.4.4.0.3	–	–	M, T, and MX Series routers.
	jnxLdpSesDown	1.3.6.1.4.1.2636.4.4.0.4	–	–	M, T, and MX Series routers.
MPLS MIB (**jnx-mpls.mib**)	**mplsLspUp** (Deprecated)	1.3.6.1.4.1.2636.3.2.4.1	–	–	
	mplsLspInfoUp	1.3.6.1.4.1.2636.3.2.0.1	–	–	M, T, and MX Series routers.
	mplsLspDown (Deprecated)	1.3.6.1.4.1.2636.3.2.4.2	–	–	
	mplsLspInfoDown	1.3.6.1.4.1.2636.3.2.0.2	–	–	M, T, and MX Series routers.
	mplsLspChange (Deprecated)	1.3.6.1.4.1.2636.3.2.4.3	–	–	
	mplsLspInfoChange	1.3.6.1.4.1.2636.3.2.0.3	–	–	M, T, and MX Series routers.
	mplsLspPathDown (Deprecated)	1.3.6.1.4.1.2636.3.2.4.4	–	–	
	mplsLspInfoPathDown	1.3.6.1.4.1.2636.3.2.0.4	–	–	M, T, and MX Series routers.
	mplsLspInfoPathUp	1.3.6.1.4.1.2636.3.2.0.5	–	–	M, T, and MX Series routers.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
VPN MIB (**jnx-vpn.mib**)	**jnxVpnIfUp**	1.3.6.1.4.1.2636.3.26.0.1	–	–	M, T, and MX Series routers.
	jnxVpnIfDown	1.3.6.1.4.1.2636.3.26.0.2	–	–	M, T, and MX Series routers.
	jnxVpnPwUp	1.3.6.1.4.1.2636.3.26.0.3	–	–	M, T, and MX Series routers.
	jnxVpnPwDown	1.3.6.1.4.1.2636.3.26.0.4	–	–	M, T, and MX Series routers.
AAA MIB (**jnx-user-aaa.mib**)	**jnxAccessAuthAddress PoolHighThreshold**	1.3.6.1.4.1.2636.3.51.1.0.5	–	–	SRX Series devices.
	jnxAccessAuthAddress PoolAbateThreshold	1.3.6.1.4.1.2636.3.51.1.0.6	–	–	SRX Series devices.
	jnxAccessAuthAddress PoolOutOfAddresses	1.3.6.1.4.1.2636.3.51.1.0.7	–	–	SRX Series devices.
	jnxAccessAuthAddress PoolOutOfMemory	1.3.6.1.4.1.2636.3.51.1.0.8	–	–	SRX Series devices.
	jnxAccessAuthService Up	1.3.6.1.4.1.2636.3.51.1.0.1	–	–	SRX Series devices.
	jnxAccessAuthService Down	1.3.6.1.4.1.2636.3.51.1.0.2	–	–	SRX Series devices.
	jnxAccessAuthServer Disabled	1.3.6.1.4.1.2636.3.51.1.0.3	–	–	SRX Series devices.
	jnxAccessAuthServer Enabled	1.3.6.1.4.1.2636.3.51.1.0.4	–	–	SRX Series devices.
	jnxJsFwAuthFailure	1.3.6.1.4.1.2636.3.39.1.2.1.0.1	–	–	SRX Series devices.

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
Access Authentication Methods MIB (**jnx-js-auth.mib**)	**jnxJsFwAuthServiceUp**	1.3.6.1.4.1.2636.3.39.1.2.1.0.2	–	–	SRX Series devices.
	jnxJsFwAuthServiceDown	1.3.6.1.4.1.2636.3.39.1.2.1.0.3	–	–	SRX Series devices.
	jnxJsFwAuthCapacityExceeded	1.3.6.1.4.1.2636.3.39.1.2.1.0.4	–	–	SRX Series devices.
	jnxJsNatAddrPool ThresholdStatus	1.3.6.1.4.1.2636.3.39.1.7.1.0.1	–	–	SRX Series devices.
Network Address Translation Resources-Monitoring MIB (**jnxNatMIB**)	**jnxNatAddrPoolUtil**	1.3.6.1.4.1.2636.3.59.1.2.1	–	–	M Series and MX Series routers
	jnxNatTrapSrcPoolName	1.3.6.1.4.1.2636.3.59.1.2.2	–	–	M Series and MX Series routers
	jnxNatAddrPoolThresholdStatus	1.3.6.1.4.1.2636.3.59.1.0.1	–	–	M Series and MX Series routers
Network Address Translation MIB (**jnx-js-nat.mib**)	**jnxJsScreen Attack**	1.3.6.1.4.1.2636.3.39.1.8.1.0.1	Warning	RT_SCREEN_ICMP, RT_SCREEN_IP, RT_SCREEN_ SESSION_LIMIT, RT_SCREEN_TCP, RT_SCREEN_UDP	SRX Series devices.
Security Screening Objects MIB (**jnx-js-screening.mib**)	**jnxJsScreenCfg Change**	1.3.6.1.4.1.2636.3.39.1.8.1.0.2	–	–	SRX Series devices.
jnxTLBMIB	tlbTrapMib	1.3.6.1.4.1.2636.4.32.0	-	-	MX Series routers

Table 36: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps *(continued)*

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
	tlbNotificationObjMib	1.3.6.1.4.1.2636.4.32.0. 1	-	-	MX Series routers
	tlbNotificationMib	1.3.6.1.4.1.2636.4.32.0. 2	-	-	MX Series routers
RMON Alarms					
RMON MIB (jnx-rmon.mib)	**jnxRmonGetOk**	1.3.6.1.4.1.2636.4.3.0.2	–	–	All devices running Junos OS.
SONET Alarms					
SONET MIB (jnx-sonet.mib)	**jnxSonetAlarm Cleared**	1.3.6.1.4.1.2636.4.6.0.2	–	–	Devices that run Junos OS and have SONET PICs installed.

RELATED DOCUMENTATION

- Standard SNMP Traps Supported by Junos OS | **490**
- Standard SNMP MIBs Supported by Junos OS | **452**
- Enterprise-Specific SNMP MIBs Supported by Junos OS | **436**
- Configuring SNMP Trap Options and Groups on a Device Running Junos OS | **585**
- Managing Traps and Informs | **432**

Customized SNMP MIBs for Syslog Traps

IN THIS SECTION

- Overview of Custom SNMP MIBs | 521
- Defining a Custom MIB for a Syslog Trap | 523
- Limitations of Using Custom SNMP Traps | 529
- Example Custom Syslog Trap | 530

SNMP syslog traps are alert messages sent from a remote SNMP-enabled device to a central collector notifying you of a component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB). The Juniper Networks enterprise-specific System Log MIB enables notification of an SNMP trap-based application when an important system log message occurs. The MIB is defined to map the syslog entry to the generic jnxSyslogTrap OID.

The jnxSyslogTrap OID is a trap based on the logs generated in the syslog. The Event process (eventd) monitors syslog and, based on the event policy **raise-trap** configuration statement for syslog events, sends all syslog events into one generic syslog-defined trap MIB, which is jnxSyslogTrap.

Using one generic MIB OID is inconvenient for customers who want to process syslog trap OID values to discover specific events because it is impossible to distinguish alarms having the same OID. But as of Junos OS Release 18.3R1, you can map a custom OID to a particular log and load it on the device dynamically.

The benefit of this feature is that because there is a way to assign specific OIDs to different types of syslog events, you can now effectively monitor for each different type of syslog event.

Overview of Custom SNMP MIBs

IN THIS SECTION

- Write the MIB File | 522
- Convert to a YANG File | 522
- CLI Commands to Use for Managing YANG Files | 522

To create a custom SNMP MIB for a syslog trap, you must complete the following tasks:

- Write the custom MIB.
- Convert the MIB file to YANG format and copy the YANG file to the device.
- Load the YANG file onto the device.

The following sections overview these steps.

Write the MIB File

Before you can map a particular log with a custom OID, you must write a custom MIB. To avoid collisions, you must define your MIB objects and traps only under the reserved roots shown in Table 37 on page 522.

Table 37: MIB Roots for Custom MIB Modules

Root	Description	OID
.iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxCustomMibRoot	Custom MIB module	.1.3.6.1.4.1.2636.3.86
.iso.org.dod.internet.private.enterprises.juniperMIB.jnxTraps.jnxCustomSyslogNotifications	Custom trap notification	.1.3.6.1.4.1.2636.4.30

Convert to a YANG File

Before loading your MIB definition onto the device, you must convert the MIB file to YANG format. The recommended way to covert the MIB file to YANG is to use the smidump v0.5.0 tool. The smidump tool is an open source application which can be installed on your laptop (see https://www.ibr.cs.tu-bs.de/projects/libsmi/smidump.html).

Once the file is in YANG format, you must copy it to the device. Then, using a CLI command, you load the into the SNMP process (snmpd). A corresponding JSON file is then generated, which snmpd parses and from it builds the database of the OID hierarchy. If some unknown tag is found, snmpd returns the appropriate error message.

CLI Commands to Use for Managing YANG Files

To load the YANG module into snmpd, use the **snmp** option with the **request system yang add** command:

```
user@host> request system yang add snmp module yang-filename package package-name
```

The ***yang-filename*** includes the absolute path.

NOTE: In order to run the **request system yang add** command, you must have super-user access.

There are two other commands for managing YANG files on devices: **show system yang package** and **request system yang delete**.

SEE ALSO

show system yang package

request system yang delete

request system yang add

Defining a Custom MIB for a Syslog Trap

In this procedure, we use the following example files:

- MIB file to convert: mib-jnx-example-custom-syslog.txt on page 525
- output: JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang on page 526

> **NOTE:** Although YANG can be written manually by referring to the example YANG provided in this documentation, we recommend you convert the MIB to YANG format using the smidump tool v0.5.0.

To define a custom MIB for a syslog trap:

1. Load your MIB onto the network management system (NMS) and check if there are any errors.

2. Invoke the smidump tool using the following command, where ***dependency-mib***, ***input-custom-mib-file***, and ***YANG-MODULE-NAME*** are variables for specific filenames:

   ```
   $ smidump -p dependency-mib input-custom-mib-file -f yang -o YANG-MODULE-NAME.yang
   ```

   For example:

   ```
   $ smidump -p mib-jnx-smi.txt mib-jnx-example-custom-syslog.txt -f yang -o
     JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang
   ```

   As output, you will get the converted YANG file **JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang.**

   Notice that the input custom MIB file **mib-jnx-example-custom-syslog.txt** is dependent on SNMPv2-SMI, JUNIPER-SMI, and IF-MIB. But since SNMPv2-SMI and IF-MIB are standard MIBs, their definitions are already present in smidump. So, the only dependent MIB file required is **mib-jnx-smi.txt**, which has module JUNIPER-SMI definitions.

3. Copy the file **JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang** to any path on the device, and copy all the dependent YANG files to the device at the following path: **/opt/lib/python2.7/site-packages/pyang/modules**.

> **NOTE:** You must convert all the dependent MIBs to YANG files and copy to these to the device.

Following are some of the standard MIBs that have been converted to YANG modules and are present in the above path: **IANAifType-MIB.yang**, **ietf-yang-types.yang**, **ietf-inet-types.yang**, **IF-MIB.yang**, **JUNIPER-SMI.yang**, **SNMPv2-TC.yang**.

4. Using the CLI, load the YANG modules into snmpd using this command:

```
user@host> request system yang add snmp module yang-filename package package-name
```

For example:

```
user@host> request system yang add snmp module
  /var/tmp/JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang package p1
```

The YANG module is converted to JSON format and goes to snmpd for parsing and creating the internal database.

5. To verify the trap based on the syslog with the newly added trap definitions is working, spoof (mimic) the trap. You can do this either using the CLI or an event policy. The following is an example of spoofing the trap using the CLI. See "Example Custom Syslog Trap" on page 530 for an example of using an event policy.

```
user@host> request snmp spoof-trap jnxExampleSyslogTrap?
Possible completions:
  <trap>               The name of the trap to spoof
  jnxExampleSyslogTrap1   (Dynamic)
  jnxExampleSyslogTrap2   (Dynamic)
  jnxExampleSyslogTrap3   (Dynamic)
```

```
user@host> request snmp spoof-trap jnxExampleSyslogTrap1
Spoof-trap request result: trap sent successfully
```

mib-jnx-example-custom-syslog.txt

```
-- ******************************************************************
-- Juniper enterprise specific custom syslog MIB.
--
-- Copyright (c) 2002-2004, 2006, Juniper Networks, Inc.
-- All rights reserved.
--
-- The contents of this document are subject to change without notice.
-- ******************************************************************

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32
  FROM SNMPv2-SMI
    jnxCustomMibRoot, jnxCustomSyslogNotifications
  FROM JUNIPER-SMI
 ifName
  FROM IF-MIB
;

jnxExampleCustomSyslog MODULE-IDENTITY
    LAST-UPDATED "201711270000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
            "Juniper Technical Assistance Center
             Juniper Networks, Inc.
             1133 Innovation Way
             Sunnyvale, CA 94089
             E-mail: support@juniper.net"
    DESCRIPTION
    "Example MIB objects for custom syslog"
    REVISION     "201711270000Z"
    DESCRIPTION
    "Initial draft"
    ::= { jnxCustomMibRoot 1 }

jnxExampleCustomSyslogMessage OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "The syslog message string."
        ::= { jnxExampleCustomSyslog 1 }
```

```
jnxExampleCustomSyslogInteger OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Example OID for adding custom Integer OID"
        ::= { jnxExampleCustomSyslog 2 }

jnxExampleSyslogTrap1 NOTIFICATION-TYPE
    OBJECTS { jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 1 occurs"
    ::= { jnxCustomSyslogNotifications 1 }

jnxExampleSyslogTrap2 NOTIFICATION-TYPE
    OBJECTS { jnxExampleCustomSyslogInteger, jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 2 occurs"
    ::= { jnxCustomSyslogNotifications 2 }

jnxExampleSyslogTrap3 NOTIFICATION-TYPE
    OBJECTS { ifName, jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 3 occurs"
    ::= { jnxCustomSyslogNotifications 3 }

END
```

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang

```
/*
 * This YANG module has been generated by smidump 0.5.0:
 *
 *      smidump -f yang JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB
 *
 * Do not edit. Edit the source file instead!
 */

module JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
```

```
namespace "urn:ietf:params:xml:ns:yang:smiv2:JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB";

prefix "juniper-example";

import IF-MIB {
  prefix "if-mib";
}

import JUNIPER-SMI {
  prefix "juniper-smi";
}

import ietf-yang-smiv2 {
  prefix "smiv2";
}

organization
 "Juniper Networks, Inc.";

contact
 "Juniper Technical Assistance Center
  Juniper Networks, Inc.
  1133 Innovation Way
  Sunnyvale, CA 94089
  E-mail: support@juniper.net";

description
 "Example MIB objects for custom syslog";

revision 2017-11-27 {
  description
   "Initial draft";
}


container JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
  config false;
}

notification jnxExampleSyslogTrap1 {
  description
   "This TRAP is reserved to be sent when event 1 occurs";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.1";
```

```
  container object-1 {

    leaf jnxExampleCustomSyslogMessage {
      type binary;
      description
       "The syslog message string.";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
}

notification jnxExampleSyslogTrap2 {
  description
   "This TRAP is reserved to be sent when event 2 occurs";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.2";

  container object-1 {

    leaf jnxExampleCustomSyslogInteger {
      type int32;
      description
       "Example OID for adding custom Integer OID";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.2";
    }
  }

  container object-2 {

    leaf jnxExampleCustomSyslogMessage {
      type binary;
      description
       "The syslog message string.";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
}

notification jnxExampleSyslogTrap3 {
  description
   "This TRAP is reserved to be sent when event 3 occurs";
```

```
    smiv2:oid "1.3.6.1.4.1.2636.4.30.3";

    container object-1 {

      leaf ifIndex {
        type leafref {
          path "/if-mib:IF-MIB/if-mib:ifTable/if-mib:ifEntry/if-mib:ifIndex";
        }
      }

      leaf ifName {
        type leafref {
          path "/if-mib:IF-MIB/if-mib:ifTable/if-mib:ifEntry/if-mib:ifName";
        }
      }
    }

    container object-2 {

      leaf jnxExampleCustomSyslogMessage {
        type binary;
        description
         "The syslog message string.";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
      }
    }
  }

  smiv2:alias "jnxExampleCustomSyslog" {
    smiv2:oid "1.3.6.1.4.1.2636.3.86.1";
  }

}
```

Limitations of Using Custom SNMP Traps

Be careful to write the event scripts in such a way that they won't trigger traps for frequently occurring syslogs. This practice avoids introducing more load on the device.

If you add an object whose access type is **readonly** or **readwrite**, that object will not be available for polling in snmp polling operations such as snmpget or snmpwalk; it will be treated as access type **notifyonly**. This is because this feature is for adding dynamic TRAP OID definitions to the device so that customer can

write scripts to send custom traps for each syslog. Access types **readonly** and **readwrite** are for snmp polling, whereas **notifyonly** is for traps.

For custom MIBs, the definition of a custom table is not supported. If you want to send a trap that has a table object as a varbind, use the already defined table in Junos MIBs rather than defining a custom table in your custom MIB.

The YANG file needs to be loaded on all the chassis nodes and Routing Engines separately. The **request system yang add** command does not automatically copy it to backup Routing Engine.

Example Custom Syslog Trap

This example custom syslog trap illustrates a use case in which the operator wants to receive traps when either of the following occur:

- A user enters the configuration mode in the CLI (event defined as **ui_dbase_login_event**)
- A user does a commit (event defined as **ui_commit**)

Before the custom syslog trap feature was supported, the only way to do this was to use jnxSyslogTrap, which has a fixed OID, for both events. With the custom syslog trap feature, you can now generate traps that have custom defined OIDs.

To define a custom syslog trap:

1. Use the sample **mib-jnx-example-custom-syslog-txt** file provided (see Sample MIB file on page 531) and convert it to **JUNIPER-EXAMPLE-CUSTOM-SYSLOIG-MIB.yang** (see Sample YANG Converted File on page 533).

   ```
   smidump -p mib-jnx-smi.txt mib-jnx-example-custom-syslog.txt -f yang -o
     JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang
   ```

2. Copy the YANG file onto your device.

3. Load the SNMP YANG file.

   ```
   root@host> request system yang add snmp package p1 module
   ~/JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang
   ```

4. Copy the slax script (see slax Script cutom_trap.slax (in /var/db/scripts/event) on page 535) to **/var/db/scripts/event** to spoof the trap .

   For ui_dbase_login_event, you will configure the enteredConfigMode trap which has the username varbind.

For ui_commit, you will configure the configCommitted trap which has the username command an comment as three varbinds.

5. Configure the trap:

```
set event-options policy custom-trap events ui_dbase_login_event
set event-options policy custom-trap events ui_commit
set event-options policy custom-trap then event-script custom-trap.slax
set event-options event-script file custom-trap.slax
```

6. Enable snmpd traceoptions and trap target to verify the traps that are sent.

```
set snmp trap-group trap-group targets ip-address
set snmp traceoptions flag all
```

7. Verify trap is working.

Sample MIB file

```
-- ****************************************************************
-- Juniper enterprise specific custom syslog MIB.
--
-- Copyright (c) 2002-2004, 2006, Juniper Networks, Inc.
-- All rights reserved.
--
-- The contents of this document are subject to change without notice.
-- ****************************************************************

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE
  FROM SNMPv2-SMI
    jnxCustomMibRoot, jnxCustomSyslogNotifications
  FROM JUNIPER-SMI
;

jnxExampleCustomSyslog MODULE-IDENTITY
    LAST-UPDATED "201806220000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
            "Juniper Technical Assistance Center
```

```
             Juniper Networks, Inc.
             1133 Innovation Way
             Sunnyvale, CA 94089
             E-mail: support@juniper.net"
    DESCRIPTION
    "Example MIB objects for custom syslog"
    REVISION     "201806220000Z"
    DESCRIPTION
    "Initial draft"
    ::= { jnxCustomMibRoot 1 }

username OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Username"
        ::= { jnxExampleCustomSyslog 1 }

command OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Executed command"
        ::= { jnxExampleCustomSyslog 2 }

comment OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Additional comment"
        ::= { jnxExampleCustomSyslog 3 }

enteredConfigMode NOTIFICATION-TYPE
    OBJECTS { username }
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user enteres config mode. "
    ::= { jnxCustomSyslogNotifications 1 }

configCommitted NOTIFICATION-TYPE
    OBJECTS { username, command, comment }
```

```
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user does config commit"
    ::= { jnxCustomSyslogNotifications 2 }

END
```

Sample YANG Converted File

```
/*
 * This YANG module has been generated by smidump 0.5.0:
 *
 *      smidump -f yang JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB
 *
 * Do not edit. Edit the source file instead!
 */

module JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {

  namespace "urn:ietf:params:xml:ns:yang:smiv2:JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB";

  prefix "juniper-example";

  import JUNIPER-SMI {
    prefix "juniper-smi";
  }

  import ietf-yang-smiv2 {
    prefix "smiv2";
  }

  organization
   "Juniper Networks, Inc.";

  contact
   "Juniper Technical Assistance Center
    Juniper Networks, Inc.
    1133 Innovation Way
    Sunnyvale, CA 94089
    E-mail: support@juniper.net";

  description
   "Example MIB objects for custom syslog";
```

```
revision 2018-06-22 {
  description
   "Initial draft";
}


container JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
  config false;
}

notification enteredConfigMode {
  description
   "This TRAP is sent when a user enteres config mode. ";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.1";

  container object-1 {

    leaf username {
      type binary;
      description
       "Username";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
}

notification configCommitted {
  description
   "This TRAP is sent when a user does config commit";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.2";

  container object-1 {

    leaf username {
      type binary;
      description
       "Username";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
```

```
    container object-2 {

      leaf command {
        type binary;
        description
         "Executed command";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.2";
      }
    }

    container object-3 {

      leaf comment {
        type binary;
        description
         "Additional comment";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.3";
      }
    }
  }

  smiv2:alias "jnxExampleCustomSyslog" {
    smiv2:oid "1.3.6.1.4.1.2636.3.86.1";
  }

}
```

slax Script cutom_trap.slax (in /var/db/scripts/event)

```
version 1.0;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";
match / {
    <event-script-results> {
        expr jcs:syslog("external.warning",event-script-input/trigger-event/id);
        var $id = event-script-input/trigger-event/id;
        if ($id == 'UI_DBASE_LOGIN_EVENT'){
            var $committing-user =
event-script-input/trigger-event/attribute-list/attribute[name=="username"]/value;
```

```
            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "enteredConfigMode";
                <variable-bindings>
                    "username=" _ $committing-user;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
        else if ($id == 'UI_COMMIT'){
           var $committing-user =
event-script-input/trigger-event/attribute-list/attribute[name=="username"]/value;

           var $committing-command =
event-script-input/trigger-event/attribute-list/attribute[name=="command"]/value;

           var $committing-comment =
event-script-input/trigger-event/attribute-list/attribute[name=="message"]/value;


            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "configCommitted";
                <variable-bindings>
                    "username=" _ $committing-user _ ", command=" _
$committing-command _ ", comment=" _ $committing-comment;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
    }
}
```

Example Custom Syslog Trap

This example custom syslog trap illustrates a use case in which the operator wants to receive traps when either of the following occur:

- A user enters the configuration mode in the CLI (event defined as **ui_dbase_login_event**)
- A user does a commit (event defined as **ui_commit**)

Before the custom syslog trap feature was supported, the only way to do this was to use jnxSyslogTrap, which has a fixed OID, for both events. With the custom syslog trap feature, you can now generate traps that have custom defined OIDs.

To define a custom syslog trap:

1. Use the sample **mib-jnx-example-custom-syslog-txt** file provided (see Sample MIB file on page 531) and convert it to **JUNIPER-EXAMPLE-CUSTOM-SYSLOIG-MIB.yang** (see Sample YANG Converted File on page 533).

   ```
   smidump -p mib-jnx-smi.txt mib-jnx-example-custom-syslog.txt -f yang -o
     JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang
   ```

2. Copy the YANG file onto your device.

3. Load the SNMP YANG file.

   ```
   root@host> request system yang add snmp package p1 module
   ~/JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang
   ```

4. Copy the slax script (see slax Script cutom_trap.slax (in /var/db/scripts/event) on page 535) to **/var/db/scripts/event** to spoof the trap .

   For ui_dbase_login_event, you will configure the enteredConfigMode trap which has the username varbind.

   For ui_commit, you will configure the configCommitted trap which has the username command an comment as three varbinds.

5. Configure the trap:

   ```
   set event-options policy custom-trap events ui_dbase_login_event
   set event-options policy custom-trap events ui_commit
   set event-options policy custom-trap then event-script custom-trap.slax
   set event-options event-script file custom-trap.slax
   ```

6. Enable snmpd traceoptions and trap target to verify the traps that are sent.

```
set snmp trap-group trap-group targets ip-address
set snmp traceoptions flag all
```

7. Verify trap is working.

Sample MIB file

```
-- ******************************************************************
-- Juniper enterprise specific custom syslog MIB.
--
-- Copyright (c) 2002-2004, 2006, Juniper Networks, Inc.
-- All rights reserved.
--
-- The contents of this document are subject to change without notice.
-- ******************************************************************

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE
  FROM SNMPv2-SMI
    jnxCustomMibRoot, jnxCustomSyslogNotifications
  FROM JUNIPER-SMI
;

jnxExampleCustomSyslog MODULE-IDENTITY
    LAST-UPDATED "201806220000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
            "Juniper Technical Assistance Center
             Juniper Networks, Inc.
             1133 Innovation Way
             Sunnyvale, CA 94089
             E-mail: support@juniper.net"
    DESCRIPTION
    "Example MIB objects for custom syslog"
    REVISION     "201806220000Z"
    DESCRIPTION
    "Initial draft"
    ::= { jnxCustomMibRoot 1 }

username OBJECT-TYPE
```

```
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Username"
        ::= { jnxExampleCustomSyslog 1 }

command OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Executed command"
        ::= { jnxExampleCustomSyslog 2 }

comment OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Additional comment"
        ::= { jnxExampleCustomSyslog 3 }

enteredConfigMode NOTIFICATION-TYPE
    OBJECTS { username }
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user enteres config mode. "
    ::= { jnxCustomSyslogNotifications 1 }

configCommitted NOTIFICATION-TYPE
    OBJECTS { username, command, comment }
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user does config commit"
    ::= { jnxCustomSyslogNotifications 2 }

END
```

Sample YANG Converted File

```
/*
 * This YANG module has been generated by smidump 0.5.0:
```

```
 *
 *      smidump -f yang JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB
 *
 * Do not edit. Edit the source file instead!
 */

module JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {

  namespace "urn:ietf:params:xml:ns:yang:smiv2:JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB";

  prefix "juniper-example";

  import JUNIPER-SMI {
    prefix "juniper-smi";
  }

  import ietf-yang-smiv2 {
    prefix "smiv2";
  }

  organization
   "Juniper Networks, Inc.";

  contact
   "Juniper Technical Assistance Center
    Juniper Networks, Inc.
    1133 Innovation Way
    Sunnyvale, CA 94089
    E-mail: support@juniper.net";

  description
   "Example MIB objects for custom syslog";

  revision 2018-06-22 {
    description
     "Initial draft";
  }


  container JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
    config false;
  }

  notification enteredConfigMode {
```

```
  description
   "This TRAP is sent when a user enteres config mode. ";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.1";

  container object-1 {

    leaf username {
      type binary;
      description
       "Username";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
}

notification configCommitted {
  description
   "This TRAP is sent when a user does config commit";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.2";

  container object-1 {

    leaf username {
      type binary;
      description
       "Username";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }

  container object-2 {

    leaf command {
      type binary;
      description
       "Executed command";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.2";
    }
  }

  container object-3 {
```

```
      leaf comment {
        type binary;
        description
         "Additional comment";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.3";
      }
    }
  }

  smiv2:alias "jnxExampleCustomSyslog" {
    smiv2:oid "1.3.6.1.4.1.2636.3.86.1";
  }

}
```

slax Script cutom_trap.slax (in /var/db/scripts/event)

```
version 1.0;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";
match / {
    <event-script-results> {
        expr jcs:syslog("external.warning",event-script-input/trigger-event/id);
        var $id = event-script-input/trigger-event/id;
        if ($id == 'UI_DBASE_LOGIN_EVENT'){
            var $committing-user =
event-script-input/trigger-event/attribute-list/attribute[name=="username"]/value;

            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "enteredConfigMode";
                <variable-bindings>
                    "username=" _ $committing-user;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
        else if ($id == 'UI_COMMIT'){
           var $committing-user =
event-script-input/trigger-event/attribute-list/attribute[name=="username"]/value;
```

```
           var $committing-command =
event-script-input/trigger-event/attribute-list/attribute[name=="command"]/value;

           var $committing-comment =
event-script-input/trigger-event/attribute-list/attribute[name=="message"]/value;


            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "configCommitted";
                <variable-bindings>
                    "username=" _ $committing-user _ ", command=" _
$committing-command _ ", comment=" _ $committing-comment;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
    }
}
```

CHAPTER 14

Configuring Basic SNMP

IN THIS CHAPTER

- Configuration Statements at the [edit snmp] Hierarchy Level | **545**
- Configuring SNMP | **550**
- Optimizing the Network Management System Configuration for the Best Results | **555**
- Configuring Options on Managed Devices for Better SNMP Response Time | **556**
- Best Practices for Configuring SNMP | **558**
- Configuring SNMP on a Device Running Junos OS | **564**
- Configuring the System Contact on a Device Running Junos OS | **566**
- Configuring the System Location for a Device Running Junos OS | **567**
- Configuring the System Description on a Device Running Junos OS | **568**
- Configuring SNMP Details | **568**
- Configuring a Different System Name | **571**
- Configuring the Commit Delay Timer | **571**
- Filtering Duplicate SNMP Requests | **572**
- Configuring SNMP Communities | **573**
- Configuring the SNMP Community String | **577**
- Examples: Configuring the SNMP Community String | **578**
- Adding a Group of Clients to an SNMP Community | **579**
- Configuring a Proxy SNMP Agent | **581**
- Configuring SNMP Traps | **583**
- Configuring SNMP Trap Options and Groups on a Device Running Junos OS | **585**
- Configuring SNMP Trap Options | **586**
- Configuring SNMP Trap Groups | **591**
- SNMP Traps Support | **594**
- Example: Configuring SNMP Trap Groups | **609**
- Configuring the Interfaces on Which SNMP Requests Can Be Accepted | **609**
- Example: Configuring Secured Access List Checking | **610**
- Filtering Interface Information Out of SNMP Get and GetNext Output | **610**
- Configuring MIB Views | **612**

- Configuring Ping Proxy MIB | **613**
- Understanding the Integrated Local Management Interface | **614**
- Utility MIB | **615**
- SNMP MIBs Support | **616**
- MIB Objects for the QFX Series | **633**
- Fabric Chassis MIB | **637**
- Monitoring RMON MIB Tables | **642**
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | **643**
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | **646**
- Example: Configuring SNMP | **648**
- Configuring RMON Alarms and Events | **652**

Configuration Statements at the [edit snmp] Hierarchy Level

This topic shows all possible configuration statements at the **[edit snmp]** hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

```
[edit]
snmp {
    alarm-management {
        alarm-list-name list-name {
            alarm-id id {
                alarm-state state {
                    description alarm-description;
                    notification-id notification-id-of-alarm;
                    resource-prefix alarm-resource-prefix;
                    varbind-index varbind-index-in-alarm-varbind-list;
                    varbind-subtree alarm-varbind-subtree;
                    varbind-value alarm-varbind-value;
                }
            }
        }
    }
    client-list client-list-name {
        ip-addresses;
    }
```

```
community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
        address <restrict>;
    }
    logical-system logical-system-name {
        routing-instance routing-instance-name;
        clients {
            address <restrict>;
        }
    }
    routing-instance routing-instance-name {
        clients {
            address <restrict>;
        }
    }
    view view-name;
}
contact contact;
description description;
engine-id {
    (local engine-id | use-default-ip-address | use-mac-address);
}
filter-duplicates;
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index;
        rising-threshold integer;
        sample-type type;
        startup-alarm alarm;
        syslog-subtag syslog-subtag;
```

```
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regular-expression>;
    flag flag;
    memory-trace;
    no-remote-trace;
    no-default-memory-trace;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
    logical-system logical-system-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
    enterprise-oid;
    logical-system logical-system-name {
        routing-instance routing-instance-name {
            source-address address;
        }
    }
    routing-instance routing-instance-name {
        source-address address;
    }
}
v3 {
    notify name {
        tag tag-name;
        type (trap | inform);
```

```
}
notify-filter profile-name {
    oid oid (include | exclude);
}
snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}
target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    retry-count number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
}
target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
usm {
    local-engine {
        user username {
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
```

```
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-none;
            }
        }
    }
    vacm {
        access {
            group group-name {
                (default-context-prefix | context-prefix context-prefiix){
                    security-model (any | usm | v1 | v2c) {
                        security-level (authentication | none | privacy) {
                            notify-view view-name;
                            read-view view-name;
                            write-view view-name;
                        }
                    }
                }
            }
        }
        security-to-group {
            security-model (usm | v1 | v2c) {
                security-name security-name {
                    group group-name;
                }
            }
        }
    }
}
view view-name {
    oid object-identifier (include | exclude);
}
}
```

Configuring SNMP

SNMP is implemented in the Junos OS Software running on the QFX Series and OCX Series products. By default, SNMP is not enabled. To enable SNMP, you must include the SNMP configuration statements at the **[edit]** hierarchy level.

To configure the minimum requirements for SNMP, include the following statements at the **[edit]** hierarchy level of the configuration:

```
[edit]
snmp {
    community public;
}
```

To configure complete SNMP features, include the following statements at the **[edit]** hierarchy level of the configuration:

```
snmp {
    client-list client-list-name {
        ip-addresses;
    }
    community community-name {
        authorization authorization;
        client-list-name client-list-name;
        clients {
            address restrict;
        }
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                clients {
                addresses;
                }
            }
        }
        routing-instance routing-instance-name {
            clients {
            addresses;
            }
        }
        view view-name;
    }
    contact contact;
    description description;
```

```
filter-duplicates;
filter-interfaces;
health-monitor {
    falling-threshold integer;
    interval seconds;
    rising-threshold integer;
}
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type;
        rising-event-index index;
        rising-threshold integer;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
    history history-index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regular-expression>;
    flag flag;
}
```

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance routing-instance-name;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);
```

```
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
usm {
    local-engine {
        user username {
            authentication-sha {
                authentication-password authentication-password;
            }
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none;
        }
    }
    remote-engine engine-id {
        user username {
            authentication-sha {
                authentication-password authentication-password;
            }
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
```

```
            privacy-none {
              privacy-password privacy-password;
            }
          }
        }
      }
      vacm {
        access {
          group group-name {
            (default-context-prefix | context-prefix context-prefix) {
              security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                  notify-view view-name;
                  read-view view-name;
                  write-view view-name;
                }
              }
            }
          }
        }
        security-to-group {
          security-model (usm | v1 | v2c) {
            security-name security-name {
              group group-name;
            }
          }
        }
      }
    }
    view view-name {
      oid object-identifier (include | exclude);
    }
  }
```

RELATED DOCUMENTATION

Understanding SNMP Implementation in Junos OS | 389

snmp | 2233

Optimizing the Network Management System Configuration for the Best Results

IN THIS SECTION

- Changing the Polling Method from Column-by-Column to Row-by-Row | 555
- Reducing the Number of Variable Bindings per PDU | 555
- Increasing Timeout Values in Polling and Discovery Intervals | 556
- Reducing Incoming Packet Rate at the snmpd | 556

You can modify your network management system configuration to optimize the response time for SNMP queries. The following sections contain a few tips on how you can configure the network management system:

Changing the Polling Method from Column-by-Column to Row-by-Row

You can configure the network management system to use the row-by-row method for SNMP data polling. It has been proven that the row-by-row and multiple row-by-multiple-row polling methods are more efficient than column-by-column polling. By configuring the network management system to use the row-by-row data polling method, you can ensure that data for only one interface is polled in a request instead of a single request polling data for multiple interfaces, as is the case with column-by-column polling. Row-by-row polling also reduces the risk of requests timing out.

Reducing the Number of Variable Bindings per PDU

By reducing the number of variable bindings per protocol data unit (PDU), you can improve the response time for SNMP requests. A request that polls for data related to multiple objects, which are mapped to different index entries, translates into multiple requests at the device-end because the subagent might have to poll different modules to obtain data that are linked to different index entries. The recommended method is to ensure that a request has only objects that are linked to one index entry instead of multiple objects linked to different index entries.

NOTE: If responses from a device are slow, avoid using the **GetBulk** option for the device, because a **GetBulk** request might contain objects that are linked to various index entries and might further increase the response time.

Increasing Timeout Values in Polling and Discovery Intervals

By increasing the timeout values for polling and discovery intervals, you can increase the queuing time at the device end and reduce the number of throttle drops that occur because of the request timing out.

Reducing Incoming Packet Rate at the snmpd

By reducing the frequency of sending SNMP requests to a device, you can reduce the risk of SNMP requests piling up at any particular device. Apart from reducing the frequency of sending SNMP requests to a device, you can also increase the polling interval, control the use of **GetNext** requests, and reduce the number of polling stations per device.

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | **389**
- Best Practices for Configuring SNMP | **558**
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | **758**
- Configuring Options on Managed Devices for Better SNMP Response Time | **556**
- Managing Traps and Informs | **432**
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | **643**

Configuring Options on Managed Devices for Better SNMP Response Time

IN THIS SECTION

- Filtering Out Duplicate SNMP Requests | **557**
- Excluding Interfaces That Are Slow in Responding to SNMP Queries | **557**

The following sections contain information about configuration options on the managed devices that can enhance SNMP performance:

Filtering Out Duplicate SNMP Requests

If a network management station retransmits a **Get**, **GetNext**, or **GetBulk** SNMP request too frequently to a device, that request might interfere with the processing of previous requests and slow down the response time of the agent. Filtering these duplicate requests improves the response time of the SNMP agent. The Junos OS enables you to filter out duplicate **Get**, **GetNext**, and **GetBulk** SNMP requests. The Junos OS uses the following information to determine if an SNMP request is a duplicate:

- Source IP address of the SNMP request
- Source UDP port of the SNMP request
- Request ID of the SNMP request

> **NOTE:** By default, filtering of duplicate SNMP requests is disabled on devices running the Junos OS.

To enable filtering of duplicate SNMP requests on devices running the Junos OS, include the **filter-duplicates** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
filter-duplicates;
```

Excluding Interfaces That Are Slow in Responding to SNMP Queries

An interface that is slow in responding to SNMP requests for interface statistics can delay kernel responses to SNMP requests. You can review the mib2d log file to find out how long the kernel takes to respond to various SNMP requests. For more information about reviewing the log file for kernel response data, see "Checking Kernel and Packet Forwarding Engine Response" under "Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS" on page 758. If you notice that a particular interface is slow in responding, and think that it is slowing down the kernel from responding to SNMP requests, exclude that interface from the SNMP queries to the device. You can exclude an interface from the SNMP queries either by configuring the **filter-interface** statement or by modifying the SNMP view settings.

The following example shows a sample configuration for excluding interfaces from the SNMP **Get**, **GetNext**, and **Set** operations:

```
[edit]
   snmp {
   filter-interfaces {
```

```
        interfaces { # exclude the specified interfaces
          interface1;
          interface2;
        }
        all-internal-interfaces; # exclude all internal interfaces
    }
}
```

The following example shows the SNMP view configuration for excluding the interface with an interface index (ifIndex) value of 312 from a request for information related to the ifTable and ifXtable objects:

```
[edit snmp]
   view test {
      oid .1 include;
      oid ifTable.1.*.312 exclude;
      oid ifXTable.1.*.312 exclude
   }
```

Alternatively, you can take the interface that is slow in responding offline.

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | 389
- Best Practices for Configuring SNMP | 558
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | 758
- Optimizing the Network Management System Configuration for the Best Results | 555
- Managing Traps and Informs | 432
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 643

Best Practices for Configuring SNMP

IN THIS SECTION

- Configuring Basic Settings for SNMPv1 and SNMPv2 | 559
- Configuring Basic Settings for SNMPv3 | 560
- Configuring System Name, Location, Description, and Contact Information | 563

The following sections contain information about basic SNMP configuration and a few examples of configuring the basic SNMP operations on devices running Junos OS:

Configuring Basic Settings for SNMPv1 and SNMPv2

By default, SNMP is not enabled on devices running Junos OS. To enable SNMP on devices running Junos OS, include the **community public** statement at the **[edit snmp]** hierarchy level.

Enabling SNMPv1 and SNMPv2 Get and GetNext Operations

```
[edit]
snmp {
    community public;
}
```

A community that is defined as public grants access to all MIB data to any client.

To enable SNMPv1 and SNMPv2 **Set** operations on the device, you must include the following statements at the **[edit snmp]** hierarchy level:

Enabling SNMPv1 and SNMPv2 Set Operations

```
[edit snmp]
view all {
    oid .1;
}
community private {
    view all;
    authorization read-write;
}
```

The following example shows the basic minimum configuration for SNMPv1 and SNMPv2 traps on a device:

Configuring SNMPv1 and SNMPv2 Traps

```
[edit snmp]
```

```
trap-group jnpr {
    targets {
        192.168.69.179;
    }
}
```

Configuring Basic Settings for SNMPv3

The following example shows the minimum SNMPv3 configuration for enabling **Get**, **GetNext**, and **Set** operations on a device (note that the configuration has authentication set to **md5** and privacy to **none**):

Enabling SNMPv3 Get, GetNext, and Set Operations

```
[edit snmp]
v3 {
    usm {
        local-engine {
            user jnpruser {
                authentication-md5 {
                    authentication-key "$9$guaDiQFnAuOQzevMWx7ikqP"; ## SECRET-DATA
                }
                privacy-none;
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name jnpruser {
                    group grpnm;
                }
            }
        }
        access {
            group grpnm {
                default-context-prefix {
                    security-model any {
                        security-level authentication {
                            read-view all;
```

```
                write-view all;
            }
        }
    }
  }
 }
 view all {
    oid .1;
 }
```

The following example shows the basic configuration for SNMPv3 informs on a device (the configuration has authentication and privacy set to **none**):

Configuring SNMPv3 Informs

```
[edit snmp]
v3 {
    usm {
        remote-engine 00000063200133a2c0a845c3 {
            user RU2_v3_sha_none {
                authentication-none;
                privacy-none;
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name RU2_v3_sha_none {
                    group g1_usm_auth;
                }
            }
        }
        access {
            group g1_usm_auth {
                default-context-prefix {
                    security-model usm {
                        security-level authentication {
```

```
                    read-view all;
                    write-view all;
                    notify-view all;
                }
            }
        }
    }
  }
  target-address TA2_v3_sha_none {
    address 192.168.69.179;
    tag-list tl1;
    address-mask 255.255.252.0;
    target-parameters TP2_v3_sha_none;
  }
  target-parameters TP2_v3_sha_none {
    parameters {
      message-processing-model v3;
      security-model usm;
      security-level none;
      security-name RU2_v3_sha_none;
    }
    notify-filter nf1;
  }
  notify N1_all_tl1_informs {
    type inform; # Replace inform with trap to convert informs to traps.
    tag tl1;
  }
  notify-filter nf1 {
    oid .1 include;
  }
}
view all {
  oid .1 include;
}
```

You can convert the SNMPv3 informs to traps by setting the value of the **type** statement at the **[edit snmp v3 notify N1_all_tl1_informs]** hierarchy level to **trap** as shown in the following example:

Converting Informs to Traps

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

Configuring System Name, Location, Description, and Contact Information

Junos OS enables you to include the name and location of the system, administrative contact information, and a brief description of the system in the SNMP configuration.

NOTE: Always keep the name, location, contact, and description information configured and updated for all your devices that are managed by SNMP.

The following example shows a typical configuration.

TIP: Use quotation marks to enclose the system name, contact, location, and description information that contain spaces.

```
[edit]
   snmp {
      name “snmp 001”; # Overrides the system name.
      contact “Juniper Berry, (650) 555 1234”; # Specifies the name and phone number of the administrator.
      location “row 11, rack C”; # Specifies the location of the device.
      description “M40 router with 8 FPCs” # Configures a description for the device.
   }
```

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | 389
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | 758
- Optimizing the Network Management System Configuration for the Best Results | 555
- Configuring Options on Managed Devices for Better SNMP Response Time | 556
- Managing Traps and Informs | 432
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 643

Configuring SNMP on a Device Running Junos OS

By default, SNMP is disabled on devices running Junos OS. To enable SNMP on a router or switch, you must include the SNMP configuration statements at the **[edit snmp]** hierarchy level.

To configure the minimum requirements for SNMP, include the following statements at the **[edit snmp]** hierarchy level of the configuration:

```
[edit]
snmp {
    community public;
}
```

The community defined here as **public** grants read access to all MIB data to any client.

To configure complete SNMP features, include the following statements at the **[edit snmp]** hierarchy level:

```
snmp {
    client-list client-list-name {
        ip-addresses;
    }
    community community-name {
        authorization authorization;
        client-list-name client-list-name;
        clients {
            address restrict;
        }
        routing-instance routing-instance-name {
            clients {
            addresses;
            }
        }
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                clients {
                addresses;
                }
            }
        }
        view view-name;
    }
    contact contact;
    description description;
    engine-id {
```

```
    (local engine-id | use-mac-address | use-default-ip-address);
}
filter-duplicates;
health-monitor {
    falling-threshold integer;
    interval seconds;
    rising-threshold integer;
}
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description text-description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index;
        sample-type type;
        startup-alarm alarm;
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description text-description;
        type type;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regular-expression>;
    flag flag;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
```

```
        targets {
            address;
        }
        version (all | v1 | v2);
    }
    trap-options {
        agent-address outgoing-interface;
        source-address address;
    }
    view view-name {
        oid object-identifier (include | exclude);
    }
}
```

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | 389

Configuring the System Contact on a Device Running Junos OS

You can specify an administrative contact for each system being managed by SNMP. This name is placed into the MIB II sysContact object. To configure a contact name, include the **contact** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
contact contact;
```

If the name contains spaces, enclose it in quotation marks (" ").

To define a system contact name that contains spaces:

```
[edit]
snmp {
    contact "Juniper Berry, (650) 555-1234";
}
```

RELATED DOCUMENTATION

Configuring the System Location for a Device Running Junos OS | 567
Configuring the System Description on a Device Running Junos OS | 568
Configuring a Different System Name | 571
Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring the System Location for a Device Running Junos OS

You can specify the location of each system being managed by SNMP. This string is placed into the MIB II sysLocation object. To configure a system location, include the **location** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
location location;
```

If the location contains spaces, enclose it in quotation marks (" ").

To specify the system location:

```
[edit]
snmp {
    location "Row 11, Rack C";
}
```

RELATED DOCUMENTATION

Configuring the System Contact on a Device Running Junos OS | 566
Configuring the System Description on a Device Running Junos OS | 568
Configuring a Different System Name | 571
Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring the System Description on a Device Running Junos OS

You can specify a description for each system being managed by SNMP. This string is placed into the MIB II sysDescription object. To configure a description, include the **description** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
description description;
```

If the description contains spaces, enclose it in quotation marks (" ").

To specify the system description:

```
[edit]
snmp {
    description "M40 router with 8 FPCs";
}
```

RELATED DOCUMENTATION

- Configuring the System Contact on a Device Running Junos OS | 566
- Configuring the System Location for a Device Running Junos OS | 567
- Configuring a Different System Name | 571
- Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring SNMP Details

You can use SNMP to store basic administrative details, such as a contact name and the location of the device. Your management system can then retrieve this information remotely, when you are troubleshooting an issue or performing an audit. In SNMP terminology, these are the sysContact, sysDescription, and sysLocation objects found within the system group of MIB-2 (as defined in RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*). You can set initial values directly in the Junos OS configuration for each system being managed by SNMP.

To set the system contact details:

1. Set the system contact details by including the **contact** statement at the **[edit snmp]** hierarchy level, or in an appropriate configuration group as shown here.

This administrative contact is placed into the MIB II sysContact object.

If the name contains spaces, enclose it in quotation marks (" ").

```
[edit groups global snmp]
user@host# set contact contact
```

For example:

```
[edit groups global snmp]
user@host# set contact "Enterprise Support, (650) 555-1234"
```

2. Configure a system description.

   This string is placed into the MIB II sysDescription object. If the description contains spaces, enclose it in quotation marks (" ").

```
[edit groups global snmp]
user@host# set description description
```

   For example:

```
[edit groups global snmp]
user@host# set description "M10i router with 8 FPCs"
```

3. Configure a system location.

   This string is placed into the MIB II sysLocation object. If the location contains spaces, enclose it in quotation marks (" ").

   To specify the system location:

```
[edit]
snmp {
    location "Row 11, Rack C";
}
```

```
[edit groups global snmp]
user@host# set location location
```

   For example:

```
[edit groups global snmp]
user@host# set location "London Corporate Office, Lab 5, Row 11, Rack C"
```

4. At the top level of the configuration, apply the configuration group.

   If you use a configuration group, you must apply it for it to take effect.

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

5. Commit the configuration.

   ```
   user@host# commit
   ```

6. To verify the configuration, enter the **show snmp mib walk system** operational-mode command.

   The **show snmp mib walk system** command performs a MIB walk through of the system table (from MIB-2 as defined in RFC 1213). The SNMP agent in Junos OS responds by printing each row in the table and its associated value. You can use the same command to perform a MIB walk through any part of the MIB tree supported by the agent.

   `user@host>` **show snmp mib walk system**

   ```
   sysDescr.0    = M10i router with 8 FPCs
   sysObjectID.0 = jnxProductNameM10i
   sysUpTime.0   = 173676474
   sysContact.0  = Enterprise Support, (650) 555-1234
   sysName.0     = host
   sysLocation.0 = London Corporate Office, Lab 5, Row 11, Rack C
   sysServices.0 = 4
   ```

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

Configuring SNMP Traps | 583

Configuring a Different System Name

Junos OS enables you to override the system name by including the **name** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
name name;
```

If the name contains spaces, enclose it in quotation marks (" ").

To specify the system name override:

```
[edit]
snmp {
    name "snmp 1";
}
```

RELATED DOCUMENTATION

- Configuring the System Contact on a Device Running Junos OS | 566
- Configuring the System Location for a Device Running Junos OS | 567
- Configuring the System Description on a Device Running Junos OS | 568
- Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring the Commit Delay Timer

When a router or switch first receives an SNMP nonvolatile **Set** request, a Junos OS XML protocol session opens and prevents other users or applications from changing the candidate configuration (equivalent to the command-line interface [CLI] **configure exclusive** command). If the router does not receive new SNMP **Set** requests within 5 seconds (the default value), the candidate configuration is committed and the Junos OS XML protocol session closes (the configuration lock is released). If the router receives new SNMP **Set** requests while the candidate configuration is being committed, the SNMP **Set** request is rejected and an error is generated. If the router receives new SNMP **Set** requests before 5 seconds have elapsed, the commit-delay timer (the length of time between when the last SNMP request is received and the commit is requested) resets to 5 seconds.

By default, the timer is set to 5 seconds. To configure the timer for the SNMP **Set** reply and start of the commit, include the **commit-delay** statement at the **[edit snmp nonvolatile]** hierarchy level:

```
[edit snmp nonvolatile]
commit-delay seconds;
```

seconds is the length of the time between when the SNMP request is received and the commit is requested for the candidate configuration. For more information about the **configure exclusive** command and locking the configuration, see the *Junos OS CLI User Guide* .

Filtering Duplicate SNMP Requests

By default, filtering duplicate **get**, **getNext**, and **getBulk** SNMP requests is disabled on devices running Junos OS. If a network management station retransmits a **Get**, **GetNext**, or **GetBulk** SNMP request too frequently to the router, that request might interfere with the processing of previous requests and slow down the response time of the agent. Filtering these duplicate requests improves the response time of the SNMP agent. Junos OS uses the following information to determine if an SNMP request is a duplicate:

- Source IP address of the SNMP request
- Source UDP port of the SNMP request
- Request ID of the SNMP request

To filter duplicate SNMP requests, include the **filter-duplicates** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
filter-duplicates;
```

RELATED DOCUMENTATION

Configuring the Interfaces on Which SNMP Requests Can Be Accepted | 609

Filtering Interface Information Out of SNMP Get and GetNext Output | 610

Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring SNMP Communities

Configuring the SNMP agent in Junos OS is a straightforward task that shares many familiar settings common to other managed devices in your network. For example, you need to configure Junos OS with an SNMP community string and a destination for traps. Community strings are administrative names that group collections of devices and the agents that are running on them together into common management domains. If a manager and an agent share the same community, they can communicate with each other. An SNMP community defines the level of authorization granted to its members, such as which MIB objects are available, which operations (read-only or read-write) are valid for those objects, and which SNMP clients are authorized, based on their source IP addresses.

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server.

To create a read-only SNMP community:

1. Enter the SNMP community used in your network.

   If the community name contains spaces, enclose it in quotation marks (" ").

   Community names must be unique.

   > **NOTE:** You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community *community-index*]** hierarchy levels.

   ```
   [edit groups global]
   user@host# set snmp community name
   ```

   This example uses the standard name **public** to create a community that gives limited read-only access.

   ```
   [edit groups global]
   user@host# set snmp community public
   ```

2. Define the authorization level for the community.

   The default authorization level for a community is **read-only**.

   To allow **Set** requests within a community, you need to define that community as **authorization read-write**. For **Set** requests, you also need to include the specific MIB objects that are accessible with read-write privileges using the **view** statement. The default view includes all supported MIB objects that are accessible with read-only privileges. No MIB objects are accessible with read-write privileges. For more information about the **view** statement, see "Configuring MIB Views" on page 612.

```
[edit groups global snmp community name]
user@host# set authorization authorization
```

This example confines the public community to read-only access. Any SNMP client (for example, an SNMP management system) that belongs to the public community can read MIB variables but cannot set (change) them.

```
[edit groups global snmp community public]
user@host# set authorization read-only
```

3. Define a list of clients in the community who are authorized to communicate with the SNMP agent in Junos OS.

   The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. List the clients by IP address and prefix. Typically, the list includes the SNMP network management system in your network or the address of your management network. If no **clients** statement is present, all clients are allowed. For ***address***, you must specify an IPv4 or IPv6 address, not a hostname.

   ```
   [edit groups global snmp community name]
   user@host# set clients address
   ```

   The following statement defines the hosts in the 192.168.1.0/24 network as being authorized in the public community.

   ```
   [edit groups global snmp community public]
   user@host# set clients 192.168.1.0/24
   ```

4. Define the clients that are not authorized within the community by specifying their IP address, followed by the **restrict** statement.

   ```
   [edit groups global snmp community name]
   user@host# set clients address resrict
   ```

   The following statement defines all other hosts as being restricted from the public community.

   ```
   [edit groups global snmp community public]
   user@host# set clients 0/0 restrict
   ```

5. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

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

6. Commit the configuration.

```
user@host# commit
```

To create a read-write SNMP community:

1. Enter the SNMP community used in your network.

```
[edit groups global]
user@host# set snmp community name
```

This example standard community string **private** to identify the community granted read-write access to the SNMP agent running on the device.

```
[edit groups global]
user@host# set snmp community private
```

2. Define the authorization level for the community.

```
[edit groups global snmp community name]
user@host# set authorization authorization
```

This example confines the public community to read-only access. Any SNMP client (for example, an SNMP management system) that belongs to the public community can read MIB variables but cannot set (change) them.

```
[edit groups global snmp community public]
user@host# set authorization read-write
```

3. Define a list of clients in the community who are authorized to make changes to the SNMP agent in Junos OS.

List the clients by IP address and prefix.

```
[edit groups global snmp community name]
```

```
user@host# set clients address
```

For example:

```
[edit groups global snmp community private]
user@host# set clients 192.168.1.15/24
user@host# set clients 192.168.1.18/24
```

4. Define the clients that are not authorized within the community by specifying their IP address, followed by the **restrict** statement.

```
[edit groups global snmp community name]
user@host# set clients address resrict
```

The following statement defines all other hosts as being restricted from the public community.

```
[edit groups global snmp community private]
user@host# set clients 0/0 restrict
```

5. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

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

6. Commit the configuration.

```
user@host# commit
```

RELATED DOCUMENTATION

Adding a Group of Clients to an SNMP Community | 579

Configuration Statements at the [edit snmp] Hierarchy Level | 545

Examples: Configuring the SNMP Community String | 578

Configuring the SNMP Community String

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string in a Junos OS configuration, include the **community** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
community name {
    authorization authorization;
    clients {
        default restrict;
        address restrict;
    }
    viewview-name;
}
```

If the community name contains spaces, enclose it in quotation marks (" ").

The default authorization level for a community is **read-only**. To allow **Set** requests within a community, you need to define that community as **authorization read-write**. For **Set** requests, you also need to include the specific MIB objects that are accessible with read-write privileges using the **view** statement. The default view includes all supported MIB objects that are accessible with read-only privileges; no MIB objects are accessible with read-write privileges. For more information about the **view** statement, see "Configuring MIB Views" on page 612.

The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. If no **clients** statement is present, all clients are allowed. For ***address***, you must specify an IPv4 address, not a hostname. Include the **default restrict** option to deny access to all SNMP clients for which access is not explicitly granted. We recommend that you always include the **default restrict** option to limit SNMP client access to the local switch.

NOTE: Community names must be unique within each SNMP system.

RELATED DOCUMENTATION

Configuring SNMP | 550

Examples: Configuring the SNMP Community String

Grant read-only access to all clients. With the following configuration, the system responds to SNMP **Get**, **GetNext**, and **GetBulk** requests that contain the community string **public**:

```
[edit]
snmp {
    community public {
        authorization read-only;
    }
}
```

Grant all clients read-write access to the ping MIB and **jnxPingMIB**. With the following configuration, the system responds to SNMP **Get**, **GetNext**, **GetBulk**, and **Set** requests that contain the community string **private** and specify an OID contained in the ping MIB or **jnxPingMIB** hierarchy:

```
[edit]
snmp {
    view ping-mib-view {
        oid pingMIB include;
        oid jnxPingMIB include;
        community private {
            authorization read-write;
            view ping-mib-view;
        }
    }
}
```

The following configuration allows read-only access to clients with IP addresses in the range **1.2.3.4/24**, and denies access to systems in the range **fe80::1:2:3:4/64**:

```
[edit]
snmp {
    community field-service {
        authorization read-only;
        clients {
            default restrict; # Restrict access to all SNMP clients not explicitly
            # listed on the following lines.
            1.2.3.4/24; # Allow access by all clients in 1.2.3.4/24 except
            fe80::1:2:3:4/64 restrict;# fe80::1:2:3:4/64.
        }
    }
```

```
}
```

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

Adding a Group of Clients to an SNMP Community

Junos OS enables you to add one or more groups of clients to an SNMP community. You can include the **client-list-name *name*** statement at the **[edit snmp community *community-name*]** hierarchy level to add all the members of the client list or prefix list to an SNMP community.

To define a list of clients, include the **client-list** statement followed by the IP addresses of the clients at the **[edit snmp]** hierarchy level:

```
[edit snmp]
   client-list client-list-name {
   ip-addresses;
}
```

You can configure a prefix list at the **[edit policy options]** hierarchy level. Support for prefix lists in the SNMP community configuration enables you to use a single list to configure the SNMP and routing policies. For more information about the **prefix-list** statement, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

To add a client list or prefix list to an SNMP community, include the **client-list-name** statement at the **[edit snmp community *community-name*]** hierarchy level:

```
[edit snmp community community-name]
client-list-name client-list-name;
```

NOTE: The client list and prefix list must not have the same name.

The following example shows how to define a client list:

```
[edit]
```

```
snmp {
    client-list clentlist1 {
        10.1.1.1/32;
        10.2.2.2/32;
    }
}
```

The following example shows how to add a client list to an SNMP community:

```
[edit]
snmp {
    community community1 {
        authorization read-only;
        client-list-name clientlist1;
    }
}
```

The following example shows how to add a prefix list to an SNMP community:

```
[edit]
policy-options {
    prefix-list prefixlist {
    10.3.3.3/32;
    10.5.5.5/32;
    }
}
snmp {
    community community2 {
    client-list-name prefixlist;
    }
}
```

RELATED DOCUMENTATION

client-list | 2144

client-list-name | 2145

Configuring a Proxy SNMP Agent

Starting with Release 12.3, Junos OS enables you to assign one of the devices in the network as a proxy SNMP agent through which the network management system (NMS) can query other devices in the network. When you configure a proxy, you can specify the names of devices to be managed through the proxy SNMP agent.

When the NMS queries the proxy SNMP agent, the NMS specifies the community name (for SNMPv1 and SNMPv2) or the context and security name (for SNMPv3) associated with the device from which it requires the information.

> **NOTE:** If you have configured authentication and privacy methods and passwords for SNMPv3, those parameters are also specified in the query for SNMPv3 information.

To configure a proxy SNMP agent and specify devices to be managed by the proxy SNMP agent, you can include the following configuration statements at the [**edit snmp**] hierarchy level:

```
proxy proxy-name{
    device-name device-name;
    logical-system logical-system {
        routing-instance routing-instance;
    }
    routing-instance routing-instance;
    <version-v1 | version-v2c> {
        snmp-community community-name;
        no-default-comm-to-v3-config;
    }
    version-v3 {
        security-name security-name;
        context context-name;
    }
}
```

- The **proxy** statement enables you to specify a unique name for the proxy configuration.
- The **version-v1**, **version-v2c**, and **version-v3** statements enable you to specify the SNMP version.
- The **no-default-comm-to-v3-config** statement is an optional statement at the [**edit snmp proxy *proxy-name* <version-v1 | version-v2c>**] hierarchy level that when included in the configuration requires you to manually configure the statements at the [**edit snmp v3 snmp-community *community-name***] and [**edit snmp v3 vacm**] hierarchy levels.

If the **no-default-comm-to-v3-config** statement is not included at the [**edit snmp proxy *proxy-name* <version-v1 | version-v2c>**] hierarchy level, the [**edit snmp v3 snmp-community *community-name***] and [**edit snmp v3 vacm**] hierarchy level configurations are automatically initialized.

- The **logical-system** and **routing-instance** statements are optional statements that enable you to specify logical system and routing instance names if you want to create proxies for logical systems or routing instances on the device.

> **NOTE:** Starting with Junos OS Release 15.2, you must configure **interface <*interface-name*>** statement at the **[edit snmp]** hierarchy level for the proxy SNMP agent.

> **NOTE:** The community and security configuration for the proxy should match the corresponding configuration on the device that is to be managed.

> **NOTE:** Because the proxy SNMP agent does not have trap forwarding capabilities, the devices that are managed by the proxy SNMP agent send the traps directly to the network management system.

You can use the **show snmp proxy** operational mode command to view proxy details on a device. The **show snmp proxy** command returns the proxy names, device names, SNMP version, community/security, and context information.

RELATED DOCUMENTATION

proxy (snmp) | 2203

Configuring SNMP Traps

Traps are unsolicited messages sent from an SNMP agent to remote network management systems or trap receivers. Many enterprises use SNMP traps as part of a fault-monitoring solution, in addition to system logging. In Junos OS, SNMP traps are not forwarded by default, so you must configure a trap-group if you wish to use SNMP traps.

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps.. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name.

To configure an SNMP trap:

1. Create a single, consistent source address that Junos OS applies to all outgoing traps in your device.

   A source address is useful, because although most Junos OS devices have a number of outbound interfaces, using one source address helps a remote NMS to associate the source of the traps with an individual device

   ```
   [edit groups global snmp]
   user@host# set trap-options source-address address
   ```

   This example uses the IP address of the loopback interface (lo0) as the source address for all the SNMP traps that originate from the device.

   ```
   [edit groups global snmp]
   user@host# set trap-options source-address lo0
   ```

2. Create a trap group in which you can list the types of traps to be forwarded and the targets (addresses) of the receiving remote management systems.

   ```
   [edit groups global snmp trap-group group-name]
   user@host# set version (all | v1 | v2) targets address
   ```

   This example creates a trap group called **managers**, allows SNMP version 2-formatted notifications (traps) to be sent to the host at address 192.168.1.15. This statement forwards all categories of traps.

   ```
   [edit groups global snmp trap-group managers]
   user@host# set version v2 targets 192.168.1.15
   ```

3. Define the specific subset of trap categories to be forwarded.

   For a list of categories, see “Configuring SNMP Trap Groups” on page 591.

```
[edit groups global snmp trap-group group-name]
user@host# set categories category
```

The following statement configures the standard MIB-II authentication failures on the agent (the device).

```
[edit groups global snmp trap-group managers]
user@host# set categories authentication
```

4. At the top level of the configuration, apply the configuration group.

   If you use a configuration group, you must apply it for it to take effect.

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

5. Commit the configuration.

```
user@host# commit
```

6. To verify the configuration, generate an authentication failure trap.

   This means that the SNMP agent received a request with an unknown community. Other traps types can also be spoofed as well.

   This feature enables you to trigger SNMP traps from routers and ensure that they are processed correctly within your existing network management infrastructure. This is also useful for testing and debugging SNMP behavior on the switch or NMS.

   Using the **monitor traffic** command, you can verify that the trap is sent to the network management system.

   `user@host>` **request snmp spoof-trap authenticationFailure**

```
Spoof-trap request result: trap sent successfully
```

RELATED DOCUMENTATION

- Adding a Group of Clients to an SNMP Community | 579
- Configuration Statements at the [edit snmp] Hierarchy Level | 545
- Examples: Configuring the SNMP Community String | 578

Configuring SNMP Trap Options and Groups on a Device Running Junos OS

Some carriers have more than one trap receiver that forwards traps to a central NMS. This allows for more than one path for SNMP traps from a router to the central NMS through different trap receivers. A device running Junos OS can be configured to send the same copy of each SNMP trap to every trap receiver configured in the trap group.

The source address in the IP header of each SNMP trap packet is set to the address of the outgoing interface by default. When a trap receiver forwards the packet to the central NMS, the source address is preserved. The central NMS, looking only at the source address of each SNMP trap packet, assumes that each SNMP trap came from a different source.

In reality, the SNMP traps came from the same router, but each left the router through a different outgoing interface.

The statements discussed in the following sections are provided to allow the NMS to recognize the duplicate traps and to distinguish SNMPv1 traps based on the outgoing interface.

To configure SNMP trap options and trap groups, include the **trap-options** and **trap-group** statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    targets {
        address;
    }
    version (all | v1 | v2);
}
```

RELATED DOCUMENTATION

Configuring SNMP Trap Options | 586

Configuring SNMP Trap Groups | 591

Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configuring SNMP Trap Options

IN THIS SECTION

- Configuring the Source Address for SNMP Traps | 587
- Configuring the Agent Address for SNMP Traps | 590
- Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps | 590

Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router to a single address regardless of the outgoing interface. In addition, you can set the agent address of the SNMPv1 traps. For more information about the contents of SNMPv1 traps, see RFC 1157.

> **NOTE:** SNMP cannot be associated with any routing instances other than the master routing instance.

To configure SNMP trap options, include the **trap-options** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-options {
   agent-address outgoing-interface;
   context-oid;
   enterprise-oid;
   logical-system logical-system-name {
      routing-instance routing-instance-name {
         source-address address;
      }
   }
   routing-instance routing-instance-name {
      source-address address;
   }
}
```

You must also configure a trap group for the trap options to take effect. For information about trap groups, see “Configuring SNMP Trap Groups” on page 591.

This topic contains the following sections:

Configuring the Source Address for SNMP Traps

You can configure the source address of trap packets in many ways: lo0, a valid IPv4 address or IPv6 address configured on one of the router interfaces, a logical-system address, or the address of a routing-instance. The value lo0 indicates that the source address of the SNMP trap packets is set to the lowest loopback address configured on the interface lo0.

> **NOTE:** If the source address is an invalid IPv4 or IPv6 address or is not configured, SNMP traps are not generated.

You can configure the source address of trap packets in one of the following formats:

- A valid IPv4 address configured on one of the router interfaces
- A valid IPv6 address configured on one of the router interfaces
- **lo0**; that is, the lowest loopback address configured on the interface lo0
- A logical-system name
- A routing-instance name

A Valid IPv4 Address As the Source Address

To specify a valid IPv4 interface address as the source address for SNMP traps on one of the router interfaces, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
source-address address;
```

address is a valid IPv4 address configured on one of the router interfaces.

A Valid IPv6 Address As the Source Address

To specify a valid IPv6 interface address as the source address for SNMP traps on one of the router interfaces, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
```

```
source-address address;
```

address is a valid IPv6 address configured on one of the router interfaces.

The Lowest Loopback Address As the Source Address

To specify the source address of the SNMP traps so that they use the lowest loopback address configured on the interface lo0 as the source address, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
source-address lo0;
```

To enable and configure the loopback address, include the **address** statement at the **[edit interfaces lo0 unit 0 family inet]** hierarchy level:

```
[edit interfaces]
lo0 {
    unit 0 {
        family inet {
            address ip-address;
        }
    }
}
```

To configure the loopback address as the source address of trap packets:

```
[edit snmp]
trap-options {
    source-address lo0;
}
trap-group "urgent-dispatcher" {
    version v2;
    categories link startup;
    targets {
        192.168.10.22;
        172.17.1.2;
    }
```

```
}
[edit interfaces]
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.1/32;
            address 127.0.0.1/32;
        }
    }
}
```

In this example, the IP address 10.0.0.1 is the source address of every trap sent from this router.

Logical System Name as the Source Address

To specify a logical system name as the source address of SNMP traps, include the **logical-system *logical-system-name*** statement at the **[edit snmp trap-options]** hierarchy level.

For example, the following configuration sets logical system name **ls1** as the source address of SNMP traps:

```
[edit snmp]
    trap-options{
    logical-system ls1;
}
```

Routing Instance Name as the Source Address

To specify a routing instance name as the source address of SNMP traps, include the **routing-instance *routing-instance-name*** statement at the **[edit snmp trap-options]** hierarchy level.

For example, the following configuration sets the routing instance name **ri1** as the source address for SNMP traps:

```
[edit snmp]
    trap-options {
    routing-instance ri1;
}
```

Configuring the Agent Address for SNMP Traps

The agent address is only available in SNMPv1 trap packets (see RFC 1157). By default, the router's default local address is not specified in the agent address field of the SNMPv1 trap. To configure the agent address, include the **agent-address** statement at the **[edit snmp trap-options]** hierarchy level. Currently, the agent address can only be the address of the outgoing interface:

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
}
```

To configure the outgoing interface as the agent address:

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
}
trap-group " urgent-dispatcher" {
    version v1;
    categories link startup;
    targets {
        192.168.10.22;
        172.17.1.2;
    }
}
```

In this example, each SNMPv1 trap packet sent has its agent address value set to the IP address of the outgoing interface.

Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps

The snmpTrapEnterprise object helps you identify the enterprise that has defined the trap. Typically, the snmpTrapEnterprise object appears as the last varbind in enterprise-specific SNMP version 2 traps. However, starting Release 10.0, Junos OS enables you to add the snmpTrapEnterprise object identifier to standard SNMP traps as well.

To add snmpTrapEnterprise to standard traps, include the **enterprise-oid** statement at the **[edit snmp trap-options]** hierarchy level. If the **enterprise-oid** statement is not included in the configuration, snmpTrapEnterprise is added only for enterprise-specific traps.

```
[edit snmp]
trap-options {
```

```
    enterprise-oid;
}
```

RELATED DOCUMENTATION

Configuring SNMP Trap Options and Groups on a Device Running Junos OS | 585

Configuring SNMP Trap Groups | 591

Configuring SNMP Trap Groups

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. The trap group must be configured for SNMP traps to be sent. To create an SNMP trap group, include the **trap-group** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
    targets {
        address;
    }
    version (all | v1 | v2);
}
```

The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, include the **destination-port** statement. The default destination port is port 162.

For each trap group that you define, you must include the **target** statement to define at least one system as the recipient of the SNMP traps in the trap group. Specify the IPv4 or IPv6 address of each recipient, not its hostname.

Specify the types of traps the trap group can receive in the **categories** statement. For information about the category to which the traps belong, see the "Standard SNMP Traps Supported by Junos OS" on page 490 and "Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500 topics.

Specify the routing instance used by the trap group in the **routing-instance** statement. All targets configured in the trap group use this routing instance.

A trap group can receive the following categories:

- **authentication**—Authentication failures
- **chassis**—Chassis or environment notifications
- **chassis-cluster**—Clustering notifications
- **configuration**—Configuration notifications
- **link**—Link-related notifications (up-down transitions, DS-3 and DS-1 line status change, IPv6 interface state change, and Passive Monitoring PIC overload)

  > **NOTE:** To send Passive Monitoring PIC overload interface traps, select the **link** trap category.

- **otn-alarms**—OTN alarm trap subcategories
- **remote-operations**—Remote operation notifications
- **rmon-alarm**—Alarm for RMON events
- **routing**—Routing protocol notifications
- **services**—Services notifications such as circuit down or up, connection down or up, CPU exceeded, alarms, and status changes.
- **sonet-alarms**—SONET/SDH alarms

  > **NOTE:** If you omit the SONET/SDH subcategories, all SONET/SDH trap alarm types are included in trap notifications.

  - **loss-of-light**—Loss of light alarm notification
  - **pll-lock**—PLL lock alarm notification
  - **loss-of-frame**—Loss of frame alarm notification
  - **loss-of-signal**—Loss of signal alarm notification
  - **severely-errored-frame**—Severely errored frame alarm notification
  - **line-ais**—Line alarm indication signal (AIS) alarm notification
  - **path-ais**—Path AIS alarm notification
  - **loss-of-pointer**—Loss of pointer alarm notification
  - **ber-defect**—SONET/SDH bit error rate alarm defect notification

- **ber-fault**—SONET/SDH error rate alarm fault notification
- **line-remote-defect-indication**—Line remote defect indication alarm notification
- **path-remote-defect-indication**—Path remote defect indication alarm notification
- **remote-error-indication**—Remote error indication alarm notification
- **unequipped**—Unequipped alarm notification
- **path-mismatch**—Path mismatch alarm notification
- **loss-of-cell**—Loss of cell delineation alarm notification
- **vt-ais**—Virtual tributary (VT) AIS alarm notification
- **vt-loss-of-pointer**—VT loss of pointer alarm notification
- **vt-remote-defect-indication**—VT remote defect indication alarm notification
- **vt-unequipped**—VT unequipped alarm notification
- **vt-label-mismatch**—VT label mismatch error notification
- **vt-loss-of-cell**—VT loss of cell delineation notification

- **startup**—System warm and cold starts
- **timing-events**—Timing events and defects notification
- **vrrp-events**—Virtual Router Redundancy Protocol (VRRP) events such as new-master or authentication failures
- **startup**—System warm and cold starts
- **vrrp-events**—Virtual Router Redundancy Protocol (VRRP) events such as new-master or authentication failures

If you include SONET/SDH subcategories, only those SONET/SDH trap alarm types are included in trap notifications.

The **version** statement allows you to specify the SNMP version of the traps sent to targets of the trap group. If you specify **v1** only, SNMPv1 traps are sent. If you specify **v2** only, SNMPv2 traps are sent. If you specify **all**, both an SNMPv1 and an SNMPv2 trap are sent for every trap condition. For more information about the **version** statement, see **version (SNMP)**.

RELATED DOCUMENTATION

Configuring SNMP Trap Options and Groups on a Device Running Junos OS | 585

Configuring SNMP Trap Options | 586

Configuring SNMP on a Device Running Junos OS | 564

Configuration Statements at the [edit snmp] Hierarchy Level | 545

Example: Configuring SNMP Trap Groups | 609

SNMP Traps Support

IN THIS SECTION

- SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis | 594
- SNMP Traps Supported on QFabric Systems | 605

The QFX Series standalone switches, QFX Series Virtual Chassis, and QFabric systems support standard SNMP traps and Juniper Networks enterprise-specific traps.

For more information, see:

SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

IN THIS SECTION

- SNMPv1 Traps | 594
- SNMPv2 Traps | 600

QFX Series standalone switches and QFX Series Virtual Chassis support SNMPv1 and v2 traps. For more information, see:

SNMPv1 Traps

QFX Series standalone switches and QFX Series Virtual Chassis support both standard SNMPv1 traps and Juniper Networks enterprise-specific SNMPv1 traps. See:

- Table 38 on page 595 for standard SNMPv1 traps.
- Table 39 on page 597 for enterprise-specific SNMPv1 traps.

The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

Table 38: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
Link Notifications						
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	linkDown	1.3.6.1.4.1.2636	2	0	Warning	SNMP_ TRAP_ LINK_DOWN
	linkUp	1.3.6.1.4.1.2636	3	0	Info	SNMP_TRAP_ LINK_UP
Remote Operations Notifications						
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	pingProbeFailed	1.3.6.1.2.1.80.0	6	1	Info	SNMP_TRAP _PING_ PROBE_ FAILED
	pingTestFailed	1.3.6.1.2.1.80.0	6	2	Info	SNMP_TRAP_ PING_TEST _FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0	6	3	Info	SNMP_TRAP_ PING_TEST_ COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0	6	1	Info	SNMP_TRAP_ TRACE_ROUTE_ PATH_CHANGE
	traceRouteTestFailed	1.3.6.1.2.1.81.0	6	2	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0	6	3	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_COMPLETED
RMON Alarms						

Table 38: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
RFC 2819a, *RMON MIB*	fallingAlarm	1.3.6.1.2.1.16	6	2	–	–
	risingAlarm	1.3.6.1.2.1.16	6	1	–	–
Routing Notifications						
BGP 4 MIB	bgpEstablished	1.3.6.1.2.1.15.7	6	1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7	6	2	–	–
OSPF TRAP MIB	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2	6	1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2	6	2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2	6	3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2	6	4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2	6	5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2	6	6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2	6	7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2	6	10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2	6	11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2	6	13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2	6	16	–	–

Table 38: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
Startup Notifications						
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	authenticationFailure	1.3.6.1.4.1.2636	4	0	Notice	SNMPD_ TRAP_ GEN_FAILURE
	coldStart	1.3.6.1.4.1.2636	0	0	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_ WARM_START
VRRP Notifications						
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	vrrpTrapNewMaster	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW MASTER_TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_ FAILURE_TRAP

Table 39: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
Chassis Notifications (Alarm Conditions)						
Chassis MIB (jnx-chassis. mib)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1	6	1	Warning	CHASSISD_ SNMP_ TRAP
	jnxFanFailure	1.3.6.1.4.1.26361	6	2	Critical	CHASSISD_ SNMP_ TRAP

Table 39: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
	jnxOverTemperature	11.4.1.2636.4.1	6	3	Alert	CHASSISD_ SNMP_ TRAP
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1	6	7	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1	6	8	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1	6	9	Warning	CHASSISD_ SNMP_ TRAP
	jnxFruOffline	1.3.6.1.4.1.2636.4.1	6	10	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1	6	11	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1	6	12	Warning	CHASSISD_ SNMP_ TRAP
	jnxPowerSupplyOk	1.3.6.1.4.1.2636.4.2	6	1	Critical	CHASSISD_ SNMP_ TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2	6	2	Critical	CHASSISD_ SNMP_ TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2	6	3	Alert	CHASSISD_ SNMP_ TRAP
Configuration Notifications						

Table 39: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
Configuration Management MIB (jnx- configmgmt. mib)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5	6	1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5	6	2	–	–
Remote Operations						
Ping MIB (jnx-ping.mib)	jnxPingRttThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	4	–	–
	jnxPingEgressStdDev ThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	9	–	–
RMON Alarms						
RMON MIB (jnx-rmon. mib)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4.3	6	1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3	6	2	–	–

SNMPv2 Traps

- Table 40 on page 600 lists the standard SNMP traps
- Table 41 on page 602 lists the Juniper Networks enterprise-specific traps

Table 40: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, *The Interfaces Group MIB*	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_LINK_UP
Remote Operations Notifications				
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	pingProbeFailed	1.3.6.1.2.1.80.0.1	Info	SNMP_TRAP_PING_PROBE_FAILED
	pingTestFailed	1.3.6.1.2.1.80.0.2	Info	SNMP_TRAP_PING_TEST_FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Info	SNMP_TRAP_PING_TEST_COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED
RMON Alarms				

Table 40: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
RFC 2819a, *RMON MIB*	fallingAlarm	1.3.6.1.2.1.16.0.1	–	–
	risingAlarm	1.3.6.1.2.1.16.0.2	–	–
Routing Notifications				
BGP 4 MIB	bgpEstablished	1.3.6.1.2.1.15.7.1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7.2	–	–
OSPF Trap MIB	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	–	–

Table 40: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Startup Notifications				
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_ WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_ GEN_FAILURE
VRRP Notifications				
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1	Warning	VRRPD_ NEWMASTER_ TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	Warning	VRRPD_AUTH_ FAILURE_ TRAP

Table 41: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Chassis (Alarm Conditions) Notifications				
Chassis MIB (mib-jnx-chassis)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1.1	Alert	CHASSISD_ SNMP_ TRAP
	jnxFanFailure	1.3.6.1.4.1.2636.4.1.2	Critical	CHASSISD_ SNMP_ TRAP
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1.3	Critical	CHASSISD_ SNMP_ TRAP

Table 41: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1.5	Notice	CHASSISD_SNMP_TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1.6	Notice	CHASSISD_SNMP_TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1.7	Notice	CHASSISD_SNMP_TRAP
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1.8	Notice	CHASSISD_SNMP_TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1.9	Warning	CHASSISD_SNMP_TRAP
	jnxFruOffline	1.3.6.1.4.1.2636.4.1.10	Notice	CHASSISD_SNMP_TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1.11	Notice	CHASSISD_SNMP_TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1.12	Notice	CHASSISD_SNMP_TRAP
	jnxPowerSupplyOK	1.3.6.1.4.1.2636.4.2.1	Critical	CHASSISD_SNMP_TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2.2	Critical	CHASSISD_SNMP_TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2.3	Alert	CHASSISD_SNMP_TRAP
Configuration Notifications				

Table 41: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Configuration Management MIB (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–
RMON Alarms				
RMON MIB (mib-jnx-rmon)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4. 3.0.1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4. 3.0.2	–	–

SNMP Traps Supported on QFabric Systems

QFabric systems support standard SNMPv2 traps and Juniper Networks enterprise-specific SNMPv2 traps.

> **NOTE:** QFabric systems do not support SNMPv1 traps.

For more information, see:

- Table 42 on page 605 for standard SNMPv2 traps
- Table 43 on page 606 for Juniper Networks enterprise-specific SNMPv2 traps

Table 42: Standard SNMPv2 Traps Supported on QFabric Systems

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, *The Interfaces Group MIB*	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_ LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_ LINK_UP
Startup Notifications				
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_ WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_ GEN_FAILURE

Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Fabric Chassis MIB (mib-jnx-fabric-chassis)	**Fabric Chassis (Alarm Conditions) Notifications**			
	jnxFabricPowerSupplyFailure	1.3.6.1.4.1.2636.4.19.1	Warning	–
	jnxFabricFanFailure	1.3.6.1.4.1.2636.4.19.2	Critical	–
	jnxFabricOverTemperature	1.3.6.1.4.1.2636.4.19.3	Alert	–
	jnxFabricRedundancySwitchover	1.3.6.1.4.1.2636.4.19.4	Notice	–
	jnxFabricFruRemoval	1.3.6.1.4.1.2636.4.19.5	Notice	–
	jnxFabricFruInsertion	1.3.6.1.4.1.2636.4.19.6	Notice	–
	jnxFabricFruPowerOff	1.3.6.1.4.1.2636.4.19.7	Notice	–
	jnxFabricFruPowerOn	1.3.6.1.4.1.2636.4.19.8	Notice	–
	jnxFabricFruFailed	1.3.6.1.4.1.2636.4.19.9	Warning	–
	jnxFabricFruOffline	1.3.6.1.4.1.2636.4.19.10	Notice	–
	jnxFabricFruOnline	1.3.6.1.4.1.2636.4.19.11	Notice	–
	jnxFabricFruCheck	1.3.6.1.4.1.2636.4.19.12	Warning	–
	jnxFabricFEBSwitchover	1.3.6.1.4.1.2636.4.19.13	Warning	–
	jnxFabricHardDiskFailed	1.3.6.1.4.1.2636.4.19.14	Warning	–
	jnxFabricHardDiskMissing	1.3.6.1.4.1.2636.4.19.15	Warning	–
	jnxFabricBootFromBackup	1.3.6.1.4.1.2636.4.19.16	Warning	–
	Fabric Chassis (Alarm Cleared Conditions) Notifications			
	jnxFabricPowerSupplyOK	1.3.6.1.4.1.2636.4.20.1	Critical	–

Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
	jnxFabricFanOK	1.3.6.1.4.1.2636.4.20.2	Critical	–
	jnxFabricTemperatureOK	1.3.6.1.4.1.2636.4.20.3	Alert	–
	jnxFabricFruOK	1.3.6.1.4.1.2636.4.20.4	–	–
QFabric MIB (mib-jnx-qf-smi)	**QFabric MIB Notifications**			
	jnxQFabricDownloadIssued	1.3.6.1.4.1.2636.3.42.1.0.1	–	–
	jnxQFabricDownloadFailed	1.3.6.1.4.1.2636.3.42.1.0.2	–	–
	jnxQFabricDownloadSucceeded	1.3.6.1.4.1.2636.3.42.1.0.3	–	–
	jnxQFabricUpgradeIssued	1.3.6.1.4.1.2636.3.42.1.0.4	–	–
	jnxQFabricUpgradeFailed	1.3.6.1.4.1.2636.3.42.1.0.5	–	–
	jnxQFabricUpgradeSucceeded	1.3.6.1.4.1.2636.3.42.1.0.6	–	–
Configuration Notifications				
Configuration Management MIB (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				

Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–

RELATED DOCUMENTATION

- SNMP MIB Explorer
- Understanding SNMP Implementation in Junos OS | **389**
- *Understanding the Implementation of SNMP on the QFabric System*
- SNMP MIBs Support | **616**

Example: Configuring SNMP Trap Groups

Set up a trap notification list named **urgent-dispatcher** for link and startup traps. This list is used to identify the network management hosts (**1.2.3.4** and **fe80::1:2:3:4**) to which traps generated by the local router should be sent. The name specified for a trap group is used as the SNMP community string when the agent sends traps to the listed targets.

```
[edit]
snmp {
    trap-group "urgent-dispatcher" {
        version v2;
        categories link startup;
        targets {
            1.2.3.4;
            fe80::1:2:3:4;
        }
    }
}
```

RELATED DOCUMENTATION

- Configuring SNMP Trap Groups | **591**
- Configuring SNMP Trap Options and Groups on a Device Running Junos OS | **585**
- Configuring SNMP Trap Options | **586**

Configuring the Interfaces on Which SNMP Requests Can Be Accepted

By default, all router or switch interfaces have SNMP access privileges. To limit the access through certain interfaces only, include the **interface** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
interface [ interface-names ];
```

Specify the names of any logical or physical interfaces that should have SNMP access privileges. Any SNMP requests entering the router or switch from interfaces not listed are discarded.

RELATED DOCUMENTATION

Example: Configuring Secured Access List Checking | 610

Example: Configuring Secured Access List Checking

SNMP access privileges are granted to only devices on interfaces **so-0/0/0** and **at-1/0/1**. The following example does this by configuring a list of logical interfaces:

```
[edit]
snmp {
    interface [ so-0/0/0.0 so-0/0/0.1 at-1/0/1.0 at-1/0/1.1 ];
}
```

The following example grants the same access by configuring a list of physical interfaces:

```
[edit]
snmp {
    interface [ so-0/0/0 at-1/0/1 ];
}
```

RELATED DOCUMENTATION

Configuring the Interfaces on Which SNMP Requests Can Be Accepted | 609
Filtering Interface Information Out of SNMP Get and GetNext Output | 610

Filtering Interface Information Out of SNMP Get and GetNext Output

Junos OS enables you to filter out information related to specific interfaces from the output of SNMP **Get** and **GetNext** requests performed on interface-related MIBs such as IF MIB, ATM MIB, RMON MIB, and the Juniper Networks enterprise-specific IF MIB.

You can use the following options of the **filter-interfaces** statement at the **[edit snmp]** hierarchy level to specify the interfaces that you want to exclude from SNMP **Get** and **GetNext** queries:

- **interfaces**—Interfaces that match the specified regular expressions.
- **all-internal-interfaces**—Internal interfaces.

```
[edit]
   snmp {
   filter-interfaces {
      interfaces {
         interface-name 1;
         interface-name 2;
      }
      all-internal-interfaces;
   }
}
```

Starting with Release 12.1, Junos OS provides an except option (**!** operator) that enables you to filter out all interfaces except those interfaces that match all the regular expressions prefixed with the **!** mark.

For example, to filter out all interfaces except the **ge** interfaces from the SNMP **get** and **get-next** results, enter the following command:

```
[edit snmp]
user@host# set filter-interfaces interfaces "!^ge-.*"
user@host# commit
```

When this is configured, Junos OS filters out all interfaces except the **ge** interfaces from the SNMP **get** and **get-next** results.

> **NOTE:** The **!** mark is supported only as the first character of the regular expression. If it appears anywhere else in a regular expression, Junos OS considers the regular expression invalid, and returns an error.

However, note that these settings are limited to SNMP operations, and the users can continue to access information related to the interfaces (including those hidden using the **filter-interfaces** options) using the appropriate Junos OS command-line interface (CLI) commands.

RELATED DOCUMENTATION

Configuring the Interfaces on Which SNMP Requests Can Be Accepted | 609

Configuring MIB Views

SNMPv3 defines the concept of MIB views in RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. MIB views provide an agent better control over who can access specific branches and objects within its MIB tree. A view consists of a name and a collection of SNMP object identifiers, which are either explicitly included or excluded. Once defined, a view is then assigned to an SNMPv3 group or SNMPv1/v2c community (or multiple communities), automatically masking which parts of the agent's MIB tree members of the group or community can (or cannot) access.

By default, an SNMP community grants read access and denies write access to all supported MIB objects (even communities configured as **authorization read-write**). To restrict or grant read or write access to a set of MIB objects, you must configure a MIB view and associate the view with a community.

To configure MIB views, include the **view** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
view view-name {
    oid object-identifier (include | exclude);
}
```

The **view** statement defines a MIB view and identifies a group of MIB objects. Each MIB object of a view has a common object identifier (OID) prefix. Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). A configuration statement uses a view to specify a group of MIB objects on which to define access. You can also use a wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, you must associate the view with a community.

To remove an OID completely, use the **delete view all oid *oid-number*** command but omit the **include** parameter.

```
[edit groups global snmp]
user@host# set view view-name oid object-identifier (include | exclude)
```

The following example creates a MIB view called ping-mib-view. The **oid** statement does not require a dot at the beginning of the object identifier. The **snmp view** statement includes the branch under the object identifier .1.3.6.1.2.1.80. This includes the entire DISMAN-PINGMIB subtree (as defined in RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*), which effectively permits access to any object under that branch.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid 1.3.6.1.2.1.80 include
```

The following example adds a second branch in the same MIB view.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid jnxPingMIB include
```

Assign a MIB view to a community that you want to control.

To associate MIB views with a community, include the **view** statement at the **[edit snmp community *community-name*]** hierarchy level:

```
[edit snmp community community-name]
view view-name;
```

For more information about the Ping MIB, see RFC 2925 and PING MIB.

RELATED DOCUMENTATION

- Configuring Ping Proxy MIB | 613
- view (Configuring a MIB View) | 2280
- view | 2279
- oid | 2194

Configuring Ping Proxy MIB

Restrict the ***ping-mib*** community to read and write access of the Ping MIB and **jnxpingMIB** only. Read or write access to any other MIB using this community is not allowed.

```
[edit snmp]
view ping-mib-view {
    oid 1.3.6.1.2.1.80 include; #pingMIB
    oid jnxPingMIB include; #jnxPingMIB
}
community ping-mib {
    authorization read-write;
    view ping-mib-view;
}
```

The following configuration prevents the ***no-ping-mib*** community from accessing Ping MIB and **jnxPingMIB** objects. However, this configuration does not prevent the ***no-ping-mib*** community from accessing any other MIB object that is supported on the device.

```
[edit snmp]
view no-ping-mib-view {
    oid 1.3.6.1.2.1.80 exclude; # deny access to pingMIB objects
    oid jnxPingMIB exclude; # deny access to jnxPingMIB objects
}
community no-ping-mib {
    authorization read-write;
    view ping-mib-view;
}
```

RELATED DOCUMENTATION

- Configuring MIB Views | **612**
- view (Configuring a MIB View) | **2280**
- oid | **2194**

Understanding the Integrated Local Management Interface

The Integrated Local Management Interface (ILMI) provides a mechanism for Asynchronous Transfer Mode (ATM)-attached devices, such as hosts, routers, and ATM switches, to transfer management information. ILMI provides bidirectional exchange of management information between two ATM interfaces across a physical connection. ILMI information is exchanged over a direct encapsulation of SNMP version 1 (RFC 1157, *A Simple Network Management Protocol*) over ATM Adaptation Layer 5 (AAL5) using a virtual path identifier/virtual channel identifier (VPI/VCI) value (VPI=0, VCI=16).

Junos OS supports only two ILMI MIB variables: **atmfMYIPNmAddress** and **atmfPortMyIfname**. For ATM1 and ATM2 intelligent queuing (IQ) interfaces, you can configure ILMI to communicate directly with an attached ATM switch to enable querying of the switch's IP address and port number.

For more information about the ILMI MIB, see **atmfMYIPNmAddress** or **atmfPortMyIfname** in the SNMP MIB Explorer.

RELATED DOCUMENTATION

Understanding Device Management Functions in Junos OS | 2

Utility MIB

The Juniper Networks enterprise-specific Utility MIB, whose object ID is {jnxUtilMibRoot 1}, defines objects for counters, integers, and strings. The Utility MIB contains one table for each of the following five data types:

- 32-bit counters
- 64-bit counters
- Signed integers
- Unsigned integers
- Octet strings

Each data type has an arbitrary ASCII name, which is defined when the data is populated, and a timestamp that shows the last time when the data instance was modified. For a downloadable version of this MIB, see *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

For information about the enterprise-specific Utility MIB objects, see the following topics:

- *jnxUtilCounter32Table*
- *jnxUtilCounter64Table*
- *jnxUtilIntegerTable*
- *jnxUtilUintTable*
- *jnxUtilStringTable*

RELATED DOCUMENTATION

Enterprise-Specific SNMP MIBs Supported by Junos OS | 436

Standard SNMP MIBs Supported by Junos OS | 452

Understanding the Implementation of SNMP on the QFabric System

SNMP MIBs Support

IN THIS SECTION

- MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis | 616
- MIBs Supported on QFabric Systems | 626

The QFX Series standalone switches, QFX Series Virtual Chassis, and QFabric systems support standard MIBs and Juniper Networks enterprise-specific MIBs.

> **NOTE:** For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer. You can use SNMP MIB Explorer to view information about various MIBs, MIB objects, and SNMP notifications supported on Juniper Networks devices

For more information, see:

MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

The QFX Series standalone switches and QFX Series Virtual Chassis support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

- Table 44 on page 617 for standard MIBs.
- Table 45 on page 623 for Juniper Networks enterprise-specific MIBs.

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

RFC	Additional Information
IEEE 802.1ab section 12.1, *Link Layer Discovery Protocol (LLDP) MIB*	Supported tables and objects: • lldpRemManAddrOID • lldpLocManAddrOID • lldpReinitDelay • lldpNotificationInterval • lldpStatsRxPortFramesDiscardedTotal • lldpStatsRxPortFramesError • lldpStatsRxPortTLVsDiscardedTotal • lldpStatsRxPortTLVsUnrecognizedTotal • lldpStatsRxPortAgeoutsTotal
IEEE 802.3ad, *Aggregation of Multiple Link Segments*	The following tables and objects are supported: • dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable • dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount) • dot3adTablesLastChanged
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*	—
RFC 1157, *A Simple Network Management Protocol (SNMP)*	—
RFC 1212, *Concise MIB Definitions*	—

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	The following areas are supported:
	• MIB II and its SNMP version 2 derivatives, including:
	  ◦ Statistics counters
	  ◦ IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, *IP Forwarding Table MIB*)
	  ◦ ipAddrTable
	  ◦ SNMP management
	  ◦ Interface management
	• SNMPv1 **Get**, **GetNext** requests, and SNMPv2 **GetBulk** request
	• Junos OS-specific secured access list
	• Master configuration keywords
	• Reconfigurations upon SIGHUP

RFC 1215, *A Convention for Defining Traps for use with the SNMP*	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, *Definitions of Managed Objects for Bridges*	—
RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*	—
RFC 1850, *OSPF Version 2 Management Information Base*	The following table, objects, and traps are not supported: • Host Table • ospfOriginateNewLsas and ospfRxNewLsas objects • ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow traps
RFC 1901, *Introduction to Community-based SNMPv2*	—
RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	—
RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*	—
RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*	—
RFC 2233, *The Interfaces Group MIB Using SMIv2*	**NOTE:** RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2287, *Definitions of System-Level Managed Objects for Applications*	The following objects are supported: • sysApplInstallPkgTable • sysApplInstallElmtTable • sysApplElmtRunTable • sysApplMapTable
RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*	—
RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)	**NOTE:** RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)	**NOTE:** RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	**NOTE:** RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	—
RFC 2579, *Textual Conventions for SMIv2*	—
RFC 2580, *Conformance Statements for SMIv2*	—
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*	—
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	Support does not include row creation, the Set operation, and the vrrpStatsPacketLengthErrors object.
RFC 2790, *Host Resources MIB*	Support is limited to the following objects: • Only hrStorageTable. The file systems **/**, **/config**, **/var**, and **/tmp** always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change. • Only the objects of the hrSystem and hrSWInstalled groups.
RFC 2819, *Remote Network Monitoring Management Information Base*	The following objects are supported: • etherStatsTable (for Ethernet interfaces only), alarmTable, eventTable, and logTable. • historyControlTable and etherHistoryTable (except the etherHistoryUtilization object).
RFC 2863, *The Interfaces Group MIB*	**NOTE:** RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2932, *IPv4 Multicast Routing MIB*	—
RFC 2933, *Internet Group Management Protocol (IGMP) MIB*	—

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 2934, *Protocol Independent Multicast MIB for IPv4*	In Junos OS, RFC 2934 is implemented based on a draft version, *pimmib.mib*, of the now standard RFC.
RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*	—
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	**NOTE:** RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3413, *Simple Network Management Protocol (SNMP) Applications*	All MIBs are supported except for the Proxy MIB.
RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*	—
RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*	—
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	—
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	—
RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*	—
RFC 4188, *Definitions of Managed Objects for Bridges*	The QFX3500 and QFX3600 switches support 802.1D STP (1998) and the following subtrees and objects only: • dot1dTp subtree—dot1dTpFdbAddress, dot1dTpFdbPort, and dot1dTpFdbStatus objects from the dot1dTpFdbTable table. • dot1dBase subtree—dot1dBasePort and dot1dBasePortIfIndex objects from the dot1dBasePortTable table. **NOTE:** On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (RFC 4363b, *Q-Bridge VLAN MIB*) when you issue the **show snmp mib walk** command. Not supported on OCX Series devices.
RFC 4293, *Management Information Base for the Internet Protocol (IP)*	Supports the ipAddrTable table only.
RFC 4318, *Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol*	Supports 802.1w and 802.1t extensions for RSTP. Not supported on OCX Series devices.
RFC 4363b, *Q-Bridge VLAN MIB*	**NOTE:** On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table (RFC 4188, *Definitions of Managed Objects for Bridges*) is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (in this MIB) when you issue the **show snmp mib walk** command. Not supported on OCX Series devices.
RFC 4444, *IS-IS MIB*	—

Table 44: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
Internet Assigned Numbers Authority, *IANAiftype Textual Convention MIB* (referenced by RFC 2233)	See http://www.iana.org/assignments/ianaiftype-mib .
Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*	—
Internet draft draft-ietf-idmr-igmp-mib-13.txt, *Internet Group Management Protocol (IGMP) MIB*	—
ESO Consortium MIB	**NOTE:** The ESO Consortium MIB has been replaced by RFC 3826. See http://www.snmp.com/eso/.

Table 45: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

MIB	Description
Alarm MIB (mib-jnx-chassis-alarm)	Provides support for alarms from the switch.
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring. Not supported on OCX Series devices.
Chassis MIB (mib-jnx-chassis)	Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and airflow) and inventory support for the chassis, Flexible PIC Concentrators (FPCs), and PICs. **NOTE:** The jnxLEDTable table has been deprecated.
Chassis Definitions for Router Model MIB (mib-jnx-chas-defines)	Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify routing and switching platforms and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often.

Table 45: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

MIB	Description
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class.
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.
Ethernet MAC MIB (mib-jnx-mac)	Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, inoctets, inframes, outoctets, and outframes on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port. Not supported on OCX Series devices.
Event MIB (mib-jnx-event)	Defines a generic trap that can be generated using an operations script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found. In Junos OS release 13.2X51-D10 or later, if you configured an event policy to raise a trap when a new SNMP trap target is added, the SNMPD_TRAP_TARGET_ADD_NOTICE trap is generated with information about the new target.
Firewall MIB (mib-jnx-firewall)	Provides support for monitoring firewall filter counters.
Host Resources MIB (mib-jnx-hostresources)	Extends the hrStorageTable object, providing a measure of the usage of each file system on the switch as a percentage. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables.

Table 45: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

MIB	Description
L2ALD MIB (mib-jnx-l2ald)	Provides information about Layer 2 Address Learning and related traps, such as the routing instance MAC limit trap and interface MAC limit trap. This MIB also provides VLAN information in the jnxL2aldVlanTable table for Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches. **NOTE:** Non-ELS EX Series switches use the VLAN MIB (jnxExVlanTable) for VLAN information instead of this MIB.
MPLS MIB (mib-jnx-mpls)	Provides MPLS information and defines MPLS notifications. **NOTE:** This MIB is not supported on the QFX5100 switch.
MPLS LDP MIB (mib-jnx-mpls-ldp)	Contains object definitions as described in RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*. **NOTE:** This MIB is not supported on the QFX5100 switch.
Ping MIB (mib-jnx-ping)	Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in pingCtlTable of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB.
RMON Events and Alarms MIB (mib-jnx-rmon)	Supports Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments the alarmTable object with additional information about each alarm. Two additional traps are also defined to indicate when problems are encountered with an alarm.
Structure of Management Information MIB (mib-jnx-smi)	Explains how the Juniper Networks enterprise-specific MIBs are structured.
System Log MIB (mib-jnx-syslog)	Enables notification of an SNMP trap-based application when an important system log message occurs.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.

Table 45: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

MIB	Description
VLAN MIB (mib-jnx-vlan)	Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients. **NOTE:** For ELS EX Series switches and QFX Series switches, VLAN information is available in the L2ALD MIB in the jnxL2aldVlanTable table instead of in the VLAN MIB For non-ELS EX Series switches, VLAN information is provided in the VLAN MIB in the jnxExVlanTable table. Not supported on OCX Series devices.

MIBs Supported on QFabric Systems

The QFabric systems support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

- Table 46 on page 626 for standard MIBs.
- Table 47 on page 631 for Juniper Networks enterprise-specific MIBs.

Table 46: Standard MIBs Supported on QFabric Systems

RFC	Additional Information
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*	—
RFC 1157, *A Simple Network Management Protocol (SNMP)*	—
RFC 1212, *Concise MIB Definitions*	—

Table 46: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	The following areas are supported:
	• MIB II and its SNMP version 2 derivatives, including:
	  ◦ Statistics counters
	  ◦ IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, *IP Forwarding Table MIB*)
	  ◦ ipAddrTable
	  ◦ SNMP management
	  ◦ Interface management
	• SNMPv1 **Get**, **GetNext** requests, and version 2 **GetBulk** request
	• Junos OS-specific secured access list
	• Master configuration keywords
	• Reconfigurations upon SIGHUP

RFC 1215, *A Convention for Defining Traps for use with the SNMP*	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, *Definitions of Managed Objects for Bridges*	—
RFC 1901, *Introduction to Community-based SNMPv2*	—
RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	**NOTE:** On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.
RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*	—

Table 46: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*	—
RFC 2233, *The Interfaces Group MIB Using SMIv2*	**NOTE:** RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863. **NOTE:** The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.
RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)	**NOTE:** RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)	**NOTE:** RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	**NOTE:** RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	—
RFC 2579, *Textual Conventions for SMIv2*	—
RFC 2580, *Conformance Statements for SMIv2*	—

Table 46: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*	The QFabric system supports the following tables only: • dot3StatsTable—There is one row with statistics for each Ethernet-like interface in the QFabric system. The dot3StatsIndex is an interface index that is unique across the system. • dot3ControlTable—There is one row in this table for each Ethernet-like interface in the QFabric system that implements the MAC control sublayer. OIDs supported are dot3ControlFunctionsSupported and dot3ControlInUnknownOpcode. • dot3PauseTable—There is one row in this table for each Ethernet-like interface in the QFabric system that supports the MAC control PAUSE function. OIDs supported are dot3PauseAdminMode, dot3PauseOperMode, dot3InPauseFrames, and dot3OutPauseFrames. **NOTE:** Scalar variables are not supported on the QFabric system.
RFC 2863, *The Interfaces Group MIB*	**NOTE:** RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863. **NOTE:** The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.
RFC 2933, *Internet Group Management Protocol (IGMP) MIB*	—
RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*	—
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	**NOTE:** RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.

Table 46: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	—
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	**NOTE:** RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	—
RFC 4188, *Definitions of Managed Objects for Bridges*	The QFabric system support is limited to the following objects: • Under the dot1dBase OID, the dot1dBasePortTable table supports only the first two columns in the table: dot1dBasePort and dot1dBasePortIfIndex. • The system does not implement the optional traps supporting dot1dNotifications (dot1dBridge 0). • Under the dot1dStp OID, supports only the dot1dStpPortTable table. Does not support the scalar variables under dot1dStp. • The system does not support scalar variables under dot1dTp, but under that, the dot1dTpFdbTable table is supported (dot1dBridge 4). • For OIDS with tables support only, scalar values that are returned by the SNMP agent may not be meaningful and are therefore not recommended for use. Not supported on OCX Series devices.
RFC 4293, *Management Information Base for the Internet Protocol (IP)*	Supports the ipAddrTable table only. On the QFabric system, supported objects in the ipAddrTable table include: ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask, ipAdEntBcastAddr, and ipAdEntReasmMaxSize. **NOTE:** On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.

Table 46: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 4363b, *Q-Bridge VLAN MIB*	The QFabric system supports the following tables only: • dot1qTpFdbTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1qFdbTable Not supported on OCX Series devices.

NOTE: QFabric-specific MIBs are not supported on OCX Series devices.

Table 47: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems

MIB	Description
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring. The QFabric system supports: • Analyzer table—jnxAnalyzerName, jnxMirroringRatio, jnxLossPriority. • Analyzer input table—jnxAnalyzerInputValue, jnxAnalyzerInputOption, jnxAnalyzerInputType. • Analyzer output table—jnx AnalyzerOutputValue, jnxAnalyzerOutputType.
Chassis MIB (mib-jnx-chassis)	**NOTE:** The Chassis MIB has been deprecated for the QFabric system. We recommend that you use the Fabric Chassis MIB (mib-jnx-fabric-chassis) for information about the QFabric system.
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class. The QFabric system supports the following tables and objects: • Jnxcosifstatflagtable—jnxCosIfstatFlags and jnxCosIfIndex. • Jnxcosqstattable—jnxCosQstatTxedPkts, jnxCosQstatTxedPktRate, jnxCosQstatTxedBytes, and jnxCosQstatTxedByteRate. • Jnxcosfcidtable—jnxCosFcIdToFcName. • Jnxcosfctable—jnxCosFcQueueNr. The QFabric system does not support any traps for this MIB.

Table 47: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems *(continued)*

MIB	Description
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable. **NOTE:** On the QFabric system, these conditions apply: • All scalar variables under the jnxCmCfgChg table are supported. • Supported scalar OIDs are jnxCmCfgChgLatestIndex, jnxCmCfgChgLatestTime, jnxCmCfgChgLatestDate, jnxCmCfgChgLatestSource, jnxCmCfgChgLatestUser, and jnxCmCfgChgMaxEventEntries. • Scalar variables under the jnxCmRescueChg table are not supported.
Fabric Chassis MIB (mib-jnx-fabric-chassis)	Provides hardware information about the QFabric system and its component devices. This MIB is based on the Juniper Networks enterprise-specific Chassis MIB but adds another level of indexing that provides information for QFabric system component devices.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables. **NOTE:** On the QFabric system, scalar variables are not supported.
Power Supply Unit MIB (mib-jnx-power-supply-unit)	Provides support for environmental monitoring of the power supply unit for the Interconnect device of the QFabric system. **NOTE:** On the QFabric system, scalar variables for the jnxPsuObjects 1 object ID in the jnxPsuScalars table are not supported.
QFabric MIB (jnx-qf-smi)	Explains how the Juniper Networks enterprise-specific QFabric MIBs are structured. Defines the MIB objects that are reported by the QFabric system and the contents of the traps that can be issued by the QFabric system.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.

RELATED DOCUMENTATION

- SNMP MIB Explorer
- Understanding SNMP Implementation in Junos OS | 389
- *Understanding the Implementation of SNMP on the QFabric System*
- SNMP Traps Support | 594

MIB Objects for the QFX Series

IN THIS SECTION

- QFX Series Standalone Switches | 633
- QFabric Systems | 634
- QFabric System QFX3100 Director Device | 634
- QFabric System QFX3008-I Interconnect Device | 635
- QFabric System QFX3600-I Interconnect Device | 636
- QFabric System Node Devices | 636

This topic lists the Juniper Networks enterprise-specific SNMP Chassis MIB definition objects for the QFX Series:

QFX Series Standalone Switches

```
jnxProductLineQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductLine      82 }
  jnxProductNameQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductName      82 }
  jnxProductModelQFXSwitch      OBJECT IDENTIFIER ::= { jnxProductModel     82 }
  jnxProductVariationQFXSwitch  OBJECT IDENTIFIER ::= { jnxProductVariation 82 }
    jnxProductQFX3500s         OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch
 1 }
    jnxProductQFX360016QS      OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch
 2 }
    jnxProductQFX350048T4QS    OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch
 3 }
    jnxProductQFX510024Q       OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch
 4 }
    jnxProductQFX510048S6Q     OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch
```

```
5 }

 jnxChassisQFXSwitch           OBJECT IDENTIFIER ::= { jnxChassis          82 }

 jnxSlotQFXSwitch              OBJECT IDENTIFIER ::= { jnxSlot             82 }
   jnxQFXSwitchSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   1 }
   jnxQFXSwitchSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   2 }
   jnxQFXSwitchSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   3 }
   jnxQFXSwitchSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   4 }
   jnxQFXSwitchSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   5 }

 jnxMediaCardSpaceQFXSwitch    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   82 }
  jnxQFXSwitchMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXSwitch
1 }
```

QFabric Systems

```
jnxProductLineQFX3000        OBJECT IDENTIFIER ::= { jnxProductLine 84 }
  jnxProductNameQFX3000         OBJECT IDENTIFIER ::= { jnxProductName 84 }
  jnxProductModelQFX3000        OBJECT IDENTIFIER ::= { jnxProductModel 84 }
  jnxProductVariationQFX3000    OBJECT IDENTIFIER ::= { jnxProductVariation 84 }
   jnxProductQFX3000-G         OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000
 1 }
   jnxProductQFX3000-M         OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000
 2 }
  jnxChassisQFX3000             OBJECT IDENTIFIER ::= { jnxChassis          84 }
```

QFabric System QFX3100 Director Device

```
jnxProductLineQFX3100 OBJECT IDENTIFIER ::= { jnxProductLine      100 }
  jnxProductNameQFX3100 OBJECT IDENTIFIER ::= { jnxProductName      100 }
  jnxProductModelQFX3100 OBJECT IDENTIFIER ::= { jnxProductModel     100 }
  jnxProductVariationQFX3100  OBJECT IDENTIFIER ::= { jnxProductVariation 100 }
  jnxChassisQFX3100     OBJECT IDENTIFIER ::= { jnxChassis          100 }

  jnxSlotQFX3100            OBJECT IDENTIFIER ::= { jnxSlot             100 }
    jnxQFX3100SlotCPU       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   1 }
    jnxQFX3100SlotMemory    OBJECT IDENTIFIER ::= { jnxSlotQFX3100   2 }
    jnxQFX3100SlotPower     OBJECT IDENTIFIER ::= { jnxSlotQFX3100   3 }
    jnxQFX3100SlotFan       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   4 }
```

```
    jnxQFX3100SlotHardDisk  OBJECT IDENTIFIER ::= { jnxSlotQFX3100   5 }
    jnxQFX3100SlotNIC       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   6 }
```

QFabric System QFX3008-I Interconnect Device

```
jnxProductLineQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      60 }
  jnxProductNameQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductName      60 }
  jnxProductModelQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     60 }

  jnxProductVariationQFXInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation
 60 }
    jnxProductQFX3008           OBJECT IDENTIFIER ::= {
jnxProductVariationQFXInterconnect 1 }    jnxProductQFXC083008        OBJECT
IDENTIFIER ::= { jnxProductVariationQFXInterconnect 2 }
    jnxProductQFX3008I          OBJECT IDENTIFIER ::= {
jnxProductVariationQFXInterconnect 3 }

  jnxChassisQFXInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          60 }

  jnxSlotQFXInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             60 }
    jnxQFXInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
1 }
    jnxQFXInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
2 }
    jnxQFXInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
3 }
    jnxQFXInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
4 }
    jnxQFXInterconnectSlotCBD   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
5 }
    jnxQFXInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect
6 }

  jnxMediaCardSpaceQFXInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace
 60 }
    jnxQFXInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= {
jnxMediaCardSpaceQFXInterconnect 1 }

  jnxMidplaneQFXInterconnect    OBJECT IDENTIFIER ::= { jnxBackplane        60 }
```

QFabric System QFX3600-I Interconnect Device

```
jnxProductLineQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      91 }
  jnxProductNameQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductName      91 }

  jnxProductModelQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     91
}
  jnxProductVariationQFXMInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation
 91 }
    jnxProductQFX3600I          OBJECT IDENTIFIER ::= {
jnxProductVariationQFXMInterconnect 1 }

  jnxChassisQFXMInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          91 }


  jnxSlotQFXMInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             91 }

    jnxQFXMInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect
  1 }
    jnxQFXMInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect
  2 }
    jnxQFXMInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect
  3 }
    jnxQFXMInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect
  4 }
    jnxQFXMInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect
  5 }

  jnxMediaCardSpaceQFXMInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace
  91 }
    jnxQFXMInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= {
jnxMediaCardSpaceQFXMInterconnect 1 }
```

QFabric System Node Devices

```
jnxProductLineQFXNode       OBJECT IDENTIFIER ::= { jnxProductLine      61 }
  jnxProductNameQFXNode       OBJECT IDENTIFIER ::= { jnxProductName      61 }
  jnxProductModelQFXNode      OBJECT IDENTIFIER ::= { jnxProductModel     61 }
  jnxProductVariationQFXNode  OBJECT IDENTIFIER ::= { jnxProductVariation 61 }
    jnxProductQFX3500         OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode
1 }
    jnxProductQFX360016Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode
```

```
3 }

  jnxChassisQFXNode           OBJECT IDENTIFIER ::= { jnxChassis          61 }

  jnxSlotQFXNode              OBJECT IDENTIFIER ::= { jnxSlot             61 }
    jnxQFXNodeSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   1 }
    jnxQFXNodeSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXNode   2 }
    jnxQFXNodeSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXNode   3 }
    jnxQFXNodeSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   4 }
    jnxQFXNodeSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   5 }

  jnxMediaCardSpaceQFXNode    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   61 }
    jnxQFXNodeMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXNode
1 }
```

RELATED DOCUMENTATION

Understanding the Implementation of SNMP on the QFabric System

Fabric Chassis MIB | **637**

Fabric Chassis MIB

The Juniper Networks enterprise-specific SNMP Fabric Chassis MIB (mib-jnx-fabric-chassis) provides hardware information about the QFabric system and its component devices in a single MIB. The Fabric Chassis MIB is based on the Juniper Networks enterprise-specific Chassis MIB that provides information for individual devices. Unlike the Chassis MIB, the Fabric Chassis MIB represents the QFabric system component devices as part of the QFabric system. Only the information from the Fabric Chassis MIB (and not from individual Chassis MIBs) is available to SNMP management clients of the QFabric system.

The Fabric Chassis MIB uses the basic information structure of the Chassis MIB, but adds another level of indexing that provides detailed information about QFabric system devices. Each physical device in a QFabric system (such as a Node device or an Interconnect device) is represented with its hardware components, including the power supply, fans, and front and rear cards.

As in other SNMP systems, the SNMP manager resides on the network management system (NMS) of the network to which the QFabric system belongs. The SNMP agent (snmpd) resides in the QFabric system Director software and is responsible for receiving and distributing all traps as well as responding to all queries from the SNMP manager. In addition, there is an SNMP subagent running in the Routing Engine of each Node group and Interconnect device. The SNMP subagent manages the information about the

component device, and that information is communicated to the SNMP agent in the Director software as needed. Traps that are generated by a Node device are sent to the SNMP agent in the Director software, which in turn processes and sends them to the target IP addresses that are defined in the SNMP configuration.

Table 48 on page 638 describes the tables and objects in the Fabric Chassis MIB.

Table 48: Fabric Chassis MIB Tables and Objects

Table or Object Name	Root OID	Description
Tables with Counterparts in the Chassis MIB		
jnxFabricContainersTable	1.3.6.1.4.1.2636.3.42.2.2.2	Provides information about different types of containers in QFabric system devices. • Containers for Interconnect devices include fan trays, power supply units, control boards, and so on. • Containers for Node devices include fan trays, power supply units, Flexible PIC Concentrator (FPC), PICs, and so on. • Containers for the Director devices include CPU, memory, fan trays, power supply units, and hard disks. The containers have a non-hierarchical or flat structure, and components in them are organized as siblings to each other.
jnxFabricContentsTable	1.3.6.1.4.1.2636.3.42.2.2.3	Contains contents that are present across all devices represented in the jnxFabricDeviceTable object. This table includes all field replaceable units (FRUs) and non-FRUs for QFabric system devices. • Contents in the Interconnect devices include fan trays and control boards. • Contents in the Node devices include fan trays and power supply units. • Contents in the Director devices include CPUs, memory, fan trays, power supply units, and hard disks, but do not include network interface cards (NICs).
jnxFabricFilledTable	1.3.6.1.4.1.2636.3.42.2.2.4	Shows the status of containers in QFabric devices. The jnxFabricFilledState object represents the state of the component: (1) unknown, (2) empty, or (3) filled. **NOTE:** The jnxFabricFilledTable object does not contain information about the Director group.

Table 48: Fabric Chassis MIB Tables and Objects *(continued)*

Table or Object Name	Root OID	Description
jnxFabricOperatingTable	1.3.6.1.4.1.2636.3.42.2.2.5	Represents different operating parameters for the contents that are populated in the jnxFabricContentsTable object. • Contents in each Node device and Interconnect device include fan trays, power supply units, FPC, PIC, and Routing Engine. • Contents in the Director device include CPUs, memory, fan trays, power supply units, and hard disks, but do not include network interface cards (NICs). The jnxFabricOperatingState object provides the state of the device: (1) unknown, (2) running, (3) ready, (4) reset, (5) runningAtFullSpeed (for fans only), (6) down, (6) off (for power supply units), or (7) standby.
jnxFabricRedundancyTable	1.3.6.1.4.1.2636.3.42.2.2.6	Represents the redundancy information that is available at different subsystem levels across the QFabric system. Information about the Routing Engines in Node devices is included, but there are no corresponding entries for Interconnect devices in this table. The jnxFabricRedundancyState object indicates the state of the subsystem: (1) unknown, (2) master, (3) backup, or (4) disabled. **NOTE:** Information about redundant Director devices, virtual machines (VMs) within Director groups, and Virtual Chassis devices is not available at this time.
jnxFabricFruTable	1.3.6.1.4.1.2636.3.42.2.2.7	Contains all FRUs for the QFabric system in the jnxFabricDeviceTable table. The FRUs are listed regardless of whether or not they are installed or online. The jnxFabricFruState object represents the state of the FRU, including online, offline, or empty, and so on. This table also contains information about each FRU, such as name, type, temperature, time last powered on, and time last powered off. **NOTE:** The jnxFabricFruTable table does not include network interface cards (NICs) on Director devices.
Table Specific to the Fabric Chassis MIB		

Table 48: Fabric Chassis MIB Tables and Objects *(continued)*

Table or Object Name	Root OID	Description
jnxFabricDeviceTable	1.3.6.1.4.1.2636.3.42.2.2.1	Contains information about all devices in the QFabric system. This table organizes scalar variables represented in the Chassis MIB into a table format for the QFabric system component devices. Columns in this table include device information such as model, device alias, and serial number. The jnxFabricDeviceIndex identifies each QFabric system device (Node device, Interconnect device, and Director device). **NOTE:** At this time, information about the Virtual Chassis is not available. **NOTE:** The following objects are not supported: • jnxFabricDeviceEntryRevision • jnxFabricDeviceEntryFirmwareRevision • jnxFabricDeviceEntryKernelMemoryUsedPercent
Scalar Variables		
The following scalar variables are supported: • jnxFabricClass • jnxFabricDescr • jnxFabricSerialNo • jnxFabricRevision • jnxFabricLastInstalled • jnxFabricContentsLastChange • jnxFabricFilledLastChange	1.3.6.1.4.1.2636.3.42.2.1	Describe the QFabric system as a whole. **NOTE:** The jnxFabricFirmwareRevision scalar variable is not supported at this time.

Table 49 on page 641 describes the SNMPv2 traps that are defined in the Fabric Chassis MIB.

NOTE: Only SNMPv2 traps are supported on the QFabric system.

Table 49: Fabric Chassis MIB SNMPv2 Traps

Trap Group and Name	Root OID	Description
jnxFabricChassisTraps group—Includes the following traps: • jnxFabricPowerSupplyFailure • jnxFabricFanFailure • jnxFabricOverTemperature • jnxFabricRedundancySwitchover • jnxFabricFruRemoval • jnxFabricFruInsertion • jnxFabricFruPowerOff • jnxFabricFruPowerOn • jnxFabricFruFailed • jnxFabricFruOffline • jnxFabricFruOnline • jnxFabricFruCheck • jnxFabricFEBSwitchover • jnxFabricHardDiskFailed • jnxFabricHardDiskMissing • jnxFabricBootFromBackup • jnxFabricHighPower	1.3.6.1.4.1.2636.4.19	Indicates an alarm condition. **NOTE:** Hardware events on the Director group are detected by scanning. As a result, a trap may not be generated until up to 30 seconds after the event has occurred. **NOTE:** The software does not distinguish between the fan removal and fan failure events on the Director group. In each case, both the jnxFabricFanFailure and jnxFabricFruFailed traps are generated.
jnxFabricChassisOKTraps group—Includes the following traps: • jnxFabricPowerSupplyOK • jnxFabricFanOK • jnxFabricTemperatureOK • jnxFabricFruOK • jnxFabricHighPowerCleared	1.3.6.1.4.1.2636.4.20	Indicates an alarm cleared condition.

For more information, see the Fabric Chassis MIB at:

https://www.juniper.net/documentation/en_US/junos13.1/topics/reference/mibs/mib-jnx-fabric-chassis.txt

RELATED DOCUMENTATION

Understanding the Implementation of SNMP on the QFabric System

Monitoring RMON MIB Tables

Purpose

Monitor remote monitoring (RMON) alarm, event, and log tables.

Action

To display the RMON tables:

```
user@switch> show snmp rmon
```

```
Alarm
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                           5 falling threshold

Event
Index  Type                        Last Event
    1  log and trap                2010-07-10 11:34:17 PDT
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2010-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2010-07-10 11:34:17 PDT
```

Meaning

The display shows that an alarm has been defined to monitor jnxRmon MIB object jnxOperatingCPU, which represents the CPU utilization of the Routing Engine. The alarm is configured to generate an event that sends an SNMP trap and adds an entry to the logTable in the RMON MIB. The log table shows that two occurrences of the event have been generated—one for rising above a threshold of 90 percent, and one for falling below a threshold of 75 percent.

RELATED DOCUMENTATION

Configuring RMON Alarms and Events | 652

show snmp rmon | 2893

show snmp rmon history | 2899

clear snmp statistics | 2860

clear snmp history | 2969

Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage

Even though the Junos OS has built-in performance metrics and monitoring options, you might need to have customized performance metrics. To make it easier for you to monitor such customized data through a standard monitoring system, the Junos OS provides you with an enterprise-specific Utility MIB that can store such data and thus extend SNMP support for managing and monitoring the data of your choice.

The enterprise-specific Utility MIB provides you with container objects of the following types: **32-bit counters**, **64-bit counters**, **signed integers**, **unsigned integers**, and **octet strings**. You can use these container MIB objects to store the data that are otherwise not supported for SNMP operations. You can populate data for these objects either by using CLI commands or with the help of Op scripts and an RPC API that can invoke the CLI commands.

The following CLI commands enable you to set and clear Utility MIB object values:

- **request snmp utility-mib set instance *name* object-type <counter | counter 64 | integer | string | unsigned integer> object-value *value***
- **request snmp utility-mib clear instance *name* object-type <counter | counter 64 | integer | string | unsigned integer>**

The **instance *name*** option of the **request snmp utility-mib <set | clear>** command specifies the name of the data instance and is the main identifier of the data. The **object-type <counter | counter 64 | integer | string | unsigned integer>** option enables you specify the object type, and the **object-value *value*** option enables you to set the value of the object.

To automate the process of populating Utility MIB data, you can use a combination of an event policy and event script. The following examples show the configuration for an event policy to run **show system buffers** every hour and to store the **show system buffers** data in Utility MIB objects by running an event script (**check-mbufs.slax**).

Event Policy Configuration

To configure an event policy that runs the **show system buffers** command every hour and invokes **check-mbufs.slax** to store the **show system buffers** data into Utility MIB objects, include the following statements at the [**edit**] hierarchy level:

```
event-options {
    generate-event {
```

```
        1-HOUR time-interval 3600;
      }
      policy MBUFS {
        events 1-HOUR;
        then {
          event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
        }
      }
      event-script {
        file check-mbufs.slax;
      }
    }
```

check-mbufs.slax Script

The following example shows the **check-mbufs.slax** script that is stored under **/var/db/scripts/event/**:

```
------ script START ------
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
    <op-script-results>{
 var $cmd = <command> "show system buffers";
        var $out = jcs:invoke($cmd);

     var $lines = jcs:break_lines($out);
     for-each ($lines) {
         if (contains(., "current/peak/max")) {
             var $pattern = "([0-9]+)/([0-9]+)/([0-9]+) mbufs";
             var $split = jcs:regex($pattern, .);
             var $result = $split[2];
```

```
            var $rpc = <request-snmp-utility-mib-set> {
                <object-type> "integer";
                <instance> "current-mbufs";
                <object-value> $result;
            }
            var $res = jcs:invoke($rpc);
               }
        }
    }
}
------ script END ------
```

You can run the following command to check the data stored in the Utility MIB as a result of the event policy and script shown in the preceding examples:

```
user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs"
= 0 jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c 03 14 2c 00 2d 07 00
user@caramels>
```

NOTE: The **show snmp mib walk** command is not available on the QFabric system, but you can use external SNMP client applications to perform this operation.

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | **389**
- Best Practices for Configuring SNMP | **558**
- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | **758**
- Optimizing the Network Management System Configuration for the Best Results | **555**
- Configuring Options on Managed Devices for Better SNMP Response Time | **556**
- Managing Traps and Informs | **432**

Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage

Even though Junos OS includes built-in performance metrics and monitoring options, you might need to have customized performance metrics. To make it easier for you to monitor such customized data through a standard monitoring system, Junos OS provides you with an enterprise-specific Utility MIB that can store such data and thus extend SNMP support for managing and monitoring the data of your choice.

The enterprise-specific Utility MIB provides you with container objects of the following types: **32-bit counters**, **64-bit counters**, **signed integers**, **unsigned integers**, and **octet strings**. You can use these container MIB objects to store the data that are otherwise not supported for SNMP operations. You can populate data for these objects either by using CLI commands or with the help of Op scripts and an RPC API that can invoke the CLI commands.

The following CLI commands enable you to set and clear Utility MIB object values:

- **request snmp utility-mib set instance *name* object-type <counter | counter 64 | integer | string | unsigned integer> object-value *value***
- **request snmp utility-mib clear instance *name* object-type <counter | counter 64 | integer | string | unsigned integer>**

The **instance *name*** option of the **request snmp utility-mib <set | clear>** command specifies the name of the data instance and is the main identifier of the data. The **object-type <counter | counter 64 | integer | string | unsigned integer>** option enables you specify the object type, and the **object-value *value*** option enables you to set the value of the object.

To automate the process of populating Utility MIB data, you can use a combination of an event policy and event script. The following examples show the configuration for an event policy to run **show system buffers** every hour and to store the **show system buffers** data in Utility MIB objects by running an event script (**check-mbufs.slax**).

Event Policy Configuration

To configure an event policy that runs the **show system buffers** command every hour and invokes **check-mbufs.slax** to store the **show system buffers** data into Utility MIB objects, include the following statements at the [**edit**] hierarchy level:

```
event-options {
    generate-event {
        1-HOUR time-interval 3600;
    }
    policy MBUFS {
        events 1-HOUR;
```

```
        then {
            event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
        }
      }
      event-script {
        file check-mbufs.slax;
      }
    }
```

check-mbufs.slax Script

The following example shows the **check-mbufs.slax** script that is stored under **/var/db/scripts/event/**:

```
------ script START ------
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
    <op-script-results>{
 var $cmd = <command> "show system buffers";
        var $out = jcs:invoke($cmd);

     var $lines = jcs:break_lines($out);
     for-each ($lines) {
         if (contains(., "current/peak/max")) {
             var $pattern = "([0-9]+)/([0-9]+)/([0-9]+) mbufs";
             var $split = jcs:regex($pattern, .);
             var $result = $split[2];

             var $rpc = <request-snmp-utility-mib-set> {
                 <object-type> "integer";
                 <instance> "current-mbufs";
                 <object-value> $result;
```

```
            }
            var $res = jcs:invoke($rpc);
               }
        }
    }
}
------ script END ------
```

You can run the following command to check the data stored in the Utility MIB as a result of the event policy and script shown in the preceding examples:

```
user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs"
= 0 jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c 03 14 2c 00 2d 07 00
user@host>
```

RELATED DOCUMENTATION

Managing Traps and Informs | 432

Example: Configuring SNMP

IN THIS SECTION

- Requirements | 649
- Overview | 649
- Configuration | 649

By default, SNMP is disabled on devices running Junos OS. This example describes the steps for configuring SNMP on the QFabric system.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- Network management system (NMS) (running the SNMP manager)
- QFabric system (running the SNMP agent) with multiple Node devices

Overview

Because SNMP is disabled by default on devices running Junos OS, you must enable SNMP on your device by including configuration statements at the **[edit snmp]** hierarchy level. At a minimum, you must configure the **community public** statement. The community defined as public grants read-only access to MIB data to any client.

If no **clients** statement is configured, all clients are allowed. We recommend that you always include the **restrict** option to limit SNMP client access to the switch.

The network topology in this example includes an NMS, a QFabric system with four Node devices, and external SNMP servers that are configured for receiving traps.

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 snmp name “snmp qfabric” description “qfabric0 switch”
set snmp location “Lab 4 Row 11” contact “qfabric-admin@qfabric0”
set snmp community public authorization read-only
set snmp client-list list0 192.168.0.0/24
set snmp community public client-list-name list0
set snmp community public clients 192.170.0.0/24 restrict
set snmp trap-group “qf-traps” destination-port 155 targets 192.168.0.100
```

Step-by-Step Procedure

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

To configure SNMP on the QFabric system:

> **NOTE:** If the name, description, location, contact, or community name contains spaces, enclose the text in quotation marks (" ").

1. Configure the SNMP system name:

   ```
   [edit snmp]
   user@switch# set name “snmp qfabric”
   ```

   > **NOTE:** The above configured SNMP system name can be accessed:
   >
   > - By doing a query with the SNMPGet on policy object identifier (OID) sysName.0.
   > - From the generic jnxSyslogTrap. To send the jnxSyslogTrap, configure the trap events at **[edit event-options policy]** hierarchy.

2. Specify a description.

   ```
   [edit snmp]
   user@switch# set description “qfabric0 system”
   ```

   This string is placed into the MIB II sysDescription object.

3. Specify the physical location of the QFabric system.

   ```
   [edit snmp]
   user@switch# set location “Lab 4 Row 11”
   ```

   This string is placed into the MIB II sysLocation object.

4. Specify an administrative contact for the SNMP system.

   ```
   [edit snmp]
   user@switch# set contact “qfabric-admin@qfabric0”
   ```

This name is placed into the MIB II sysContact object.

5. Specify a unique SNMP community name and the read-only authorization level.

   NOTE: The **read-write** option is not supported on the QFabric system.

   ```
   [edit snmp]
   user@switch# set community public authorization read-only
   ```

6. Create a client list with a set of IP addresses that can use the SNMP community.

   ```
   [edit snmp]
   user@switch# set client-list list0 192.168.0.0/24
   user@switch# set community public client-list-name list0
   ```

7. Specify IP addresses of clients that are restricted from using the community.

   ```
   [edit snmp]
   user@switch# set community public clients 198.51.100.0/24 restrict
   ```

8. Configure a trap group, destination port, and a target to receive the SNMP traps in the trap group.

   ```
   [edit snmp]
   user@switch# set trap-group “qf-traps” destination-port 155 targets 192.168.0.100
   ```

   NOTE: You do not need to include the **destination-port** statement if you use the default port 162.

   The trap group qf-traps is configured to send traps to 192.168.0.100.

Results

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

```
[edit]
```

```
user@switch# show
    snmp {
        name "snmp qfabric";
        description "qfabric0 system";
        location "Lab 4 Row 11";
        contact "qfabric-admin@qfabric0";
        client-list list0 {
            192.168.0.0/24;
        }
        community public {
            authorization read-only;
            clients {
                198.51.100.0/24 restrict;
            }
        }
        trap-group qf-traps {
            destination-port 155;
            targets {
                192.168.0.100;
            }
        }
    }
```

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

RELATED DOCUMENTATION

Understanding the Implementation of SNMP on the QFabric System

snmp | 2233

Configuring RMON Alarms and Events

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds.

When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

To configure RMON alarms and events using the CLI, perform these tasks:

1. Configuring SNMP | 653
2. Configuring an Event | 654
3. Configuring an Alarm | 654

Configuring SNMP

To configure SNMP:

1. Grant read-only access to all SNMP clients:

   ```
   [edit snmp]
   user@switch# set community community-name authorization authorization
   ```

   For example:

   ```
   [edit snmp]
   user@switch# set community public authorization read-only
   ```

2. Grant read-write access to the RMON and jnx-rmon MIBs:

   ```
   [edit snmp]
   user@switch# set view view-name oid object-identifier include
   user@switch# set view view-name oid object-identifier include
   user@switch# set community community-name authorization authorization view view-name
   ```

   For example:

   ```
   [edit snmp]
   user@switch# set view rmon-mib-view oid .1.3.6.1.2.1.16 include
   user@switch# set view rmon-mib-view oid .1.3.6.1.4.1.2636.13 include
   user@switch# set community private authorization read-write view rmon-mib-view
   ```

   OIDs 1.3.6.1.2.1.16 and 1.3.6.1.4.1.2636.13 correspond to the RMON and jnxRmon MIBs.

3. Configure an SNMP trap group:

   ```
   [edit snmp]
   user@switch# set trap-group group-name categories category
   ```

```
user@switch# set trap-group group-name targets address
```

For example:

```
[edit snmp]
user@switch# set trap-group rmon-trap-group categories rmon-alarm
user@switch# set trap-group rmon-trap-group targets 192.168.5.5
```

The trap group rmon-trap-group is configured to send RMON traps to 192.168.5.5.

Configuring an Event

To configure an event:

1. Configure an event index, community name, and type:

   ```
   [edit snmp rmon]
   user@switch# set event index community community-name  typetype
   ```

   For example:

   ```
   [edit snmp rmon]
   user@switch# set event 1 community rmon-trap-group type log-and-trap
   ```

   The event community corresponds to the SNMP trap group and is not the same as an SNMP community. This event generates an SNMP trap and adds an entry to the logTable in the RMON MIB.

2. Configure a description for the event:

   ```
   [edit snmp rmon]
   user@switch# set event index description description
   ```

   For example:

   ```
   [edit snmp rmon]
   user@switch# set event 1 description “rmon event”
   ```

Configuring an Alarm

To configure an alarm:

1. Configure an alarm index, the variable to monitor, the rising and falling thresholds, and the corresponding rising and falling events:

```
[edit snmp rmon]
user@switch# set alarm index variable oid-variable falling-threshold integer rising-threshold integer
rising-event-index index falling-event-index index
```

For example:

```
[edit snmp rmon]
user@switch# set alarm 5 variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 falling-threshold 75
rising-threshold 90 rising-event-index 1 falling-event-index 1
```

The variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 corresponds to the jnxRmon MIB object jnxOperatingCPU, which represents the CPU utilization of the Routing Engine. The falling and rising threshold integers are 75 and 90. The rising and falling events both generate the same event (event index 1).

2. Configure the sample interval and type and the alarm type:

```
[edit snmp rmon]
user@switch# set alarm index interval seconds sample-type (absolute-value | delta-value)
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm)
```

For example:

```
[edit snmp rmon]
user@switch# set alarm 5 interval 30 sample-type absolute-value startup-alarm rising-or-falling-alarm
```

The absolute value of the monitored variable is sampled every 30 seconds. The initial alarm can occur because of rising above the rising threshold or falling below the falling threshold.

RELATED DOCUMENTATION

- Configuring SNMP | 550
- *Juniper Networks Enterprise-Specific MIBs*
- Monitoring RMON MIB Tables | 642
- RMON MIB Event, Alarm, Log, and History Control Tables | 781
- Understanding RMON | 774

CHAPTER 15

Configuring SNMPv3

IN THIS CHAPTER

- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Example: SNMPv3 Configuration | **658**
- Creating SNMPv3 Users | **662**
- Example: Creating SNMPv3 Users | **664**
- Configuring the SNMPv3 Authentication Type | **665**
- Configuring the SNMPv3 Encryption Type | **667**
- Defining Access Privileges for an SNMP Group | **669**
- Configuring the Access Privileges Granted to a Group | **671**
- Example: Configuring the Access Privileges Granted to a Group | **674**
- Assigning Security Model and Security Name to a Group | **676**
- Example: Security Group Configuration | **678**
- Configuring SNMPv3 Traps on a Device Running Junos OS | **678**
- Configuring the SNMPv3 Trap Notification | **680**
- Example: Configuring SNMPv3 Trap Notification | **681**
- Configuring the Trap Notification Filter | **682**
- Configuring the Trap Target Address | **683**
- Example: Configuring the Tag List | **687**
- Defining and Configuring the Trap Target Parameters | **688**
- Configuring SNMP Informs | **692**
- Configuring the Inform Notification Type and Target Address | **693**
- Example: Configuring the Inform Notification Type and Target Address | **695**
- Configuring the Remote Engine and Remote User | **696**
- Example: Configuring the Remote Engine ID and Remote User | **697**
- Configuring the Local Engine ID | **701**
- Configuring the SNMPv3 Community | **703**
- Example: Configuring an SNMPv3 Community | **706**

Minimum SNMPv3 Configuration on a Device Running Junos OS

To configure the minimum requirements for SNMPv3, include the following statements at the **[edit snmp v3]** and **[edit snmp]** hierarchy levels:

> **NOTE:** You must configure at least one view (notify, read, or write) at the **[edit snmp view-name]** hierarchy level.

```
[edit snmp]
view view-name {
    oid object-identifier (include | exclude);
}
[edit snmp v3]
notify name {
    tag tag-name;
}
notify-filter profile-name {
    oid object-identifier (include | exclude);
}
snmp-community community-index {
    security-name security-name;
}
target-address target-address-name {
    address address;
    target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
usm {
    local-engine {
        user username {
        }
    }
}
```

```
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix){
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c) {
            security-name security-name {
                group group-name;
            }
        }
    }
}
```

RELATED DOCUMENTATION

- Creating SNMPv3 Users | 662
- Configuring MIB Views | 612
- Defining Access Privileges for an SNMP Group | 669
- Configuring SNMPv3 Traps on a Device Running Junos OS | 678
- Configuring SNMP Informs | 692
- Example: SNMPv3 Configuration | 658

Example: SNMPv3 Configuration

Define an SNMPv3 configuration:

```
[edit snmp]
engine-id {
```

```
    use-mac-address;
}
view jnxAlarms {
    oid 1.3.6.1.4.1.2636.3.4 include;
}
view interfaces {
    oid 1.3.6.1.2.1.2 include;
}
view ping-mib {
    oid 1.3.6.1.2.1.80 include;
}
[edit snmp v3]
notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap;# Defines type of notification
}
notify n2 {
    tag host1;
    type trap;
}
notify-filter nf1 {
    oid .1 include; # Defines which traps to send
} # In this case, includes all traps
notify-filter nf2 {
    oid 1.3.6.1.4.1 include; # Sends enterprise-specific traps only
}
notify-filter nf3 {
    oid 1.3.6.1.2.1.1.5 include; # Sends BGP traps only
}
snmp-community index1 {
    community-name "$9$JOZi.QF/AtOz3"; # SECRET-DATA
    security-name john; # Matches the security name at the target parameters
    tag host1; # Finds the addresses that are allowed to be used with
}
target-address ta1 {# Associates the target address with the group
                # san-francisco.
    address 10.1.1.1;
    address-mask 255.255.255.0; # Defines the range of addresses
    port 162;
    tag-list router1;
    target-parameters tp1; # Applies configured target parameters
}
target-address ta2 {
    address 10.1.1.2;
```

```
    address-mask 255.255.255.0;
    port 162;
    tag-list host1;
    target-parameters tp2;
}
target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list “router1 host1”;
    target-parameters tp3;
}
target-parameters tp1 { # Defines the target parameters
    notify-filter nf1; # Specifies which notify filter to apply
    parameters {
        message-processing-model v1;
        security-model v1;
        security-level none;
        security-name john; # Matches the security name configured at the
    } # [edit snmp v3 snmp-community community-index hierarchy level.
}
target-parameters tp2 {
    notify-filter nf2;
    parameters {
        message-processing-model v1;
        security-model v1;
        security-level none;
        security-name john;
    }
}
target-parameters tp3 {
    notify-filter nf3;
    parameters {
        message-processing-model v1;
        security-model v1;
        security-level none;
        security-name john;
    }
}
usm {
    local-engine { # Defines authentication and encryption for SNMPv3 users
        user john { # security-name john is defined here
            authentication-md5 {
                authentication-password authentication-password;
```

```
            }
            privacy-des {
                privacy-password privacy-password;
            }
        }
        user bob { # security-name bob is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
        user julia { # security-name julia is defined here
            authentication-none;
            privacy-none;
        }
        user lauren { # security-name lauren is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
        }
        user richard { # security-name richard is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
    }
}
vacm {
    access {
        group san-francisco { #Defines the access privileges for the group
            default-context-prefix { # called san-francisco
                security-model v1 {
                    security-level none {
                        notify-view ping-mib;
                        read-view interfaces;
                        write-view jnxAlarms;
                    }
                }
            }
        }
```

```
    }
    security-to-group {
        security-model v1 {
            security-name john { # Assigns john to security group san-fancisco
                group san-francisco;
            }
            security-name bob { # Assigns bob to security group new-york
                group new-york;
            }
            security-name julia {# Assigns julia to security group chicago
                group chicago;
            }
            security-name lauren {# Assigns lauren to security group paris
                group paris;
            }
            security-name richard {# Assigns richard to security group geneva
                group geneva;
            }
        }
    }
}
```

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Creating SNMPv3 Users

For each SNMPv3 user, you can specify the username, authentication type, authentication password, privacy type, and privacy password. After a user enters a password, a key based on the engine ID and password is generated and is written to the configuration file. After the generation of the key, the password is deleted from this configuration file.

NOTE: You can configure only one encryption type for each SNMPv3 user.

To create users, include the **user** statement at the **[edit snmp v3 usm local-engine]** hierarchy level:

```
[edit snmp v3 usm local-engine]
user username;
```

username is the name that identifies the SNMPv3 user.

To configure user authentication and encryption, include the following statements at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-md5 {
    authentication-password authentication-password;
}
authentication-sha {
    authentication-password authentication-password;
}
authentication-none;
privacy-aes128 {
    privacy-password privacy-password;
}
privacy-des {
    privacy-password privacy-password;
}
privacy-3des {
    privacy-password privacy-password;
}
privacy-none;
```

RELATED DOCUMENTATION

- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Example: Creating SNMPv3 Users | **664**
- Example: SNMPv3 Configuration | **658**

Example: Creating SNMPv3 Users

Define SNMPv3 users:

```
[edit]
snmp {
    v3 {
        usm {
            local-engine {
                user user1 {
                    authentication-md5 {
                        authentication-password authentication-password;
                    }
                    privacy-des {
                        privacy-password password;
                    }
                }
                user user2 {
                    authentication-sha {
                        authentication-password authentication-password;
                    }
                    privacy-none;
                }
                user user3 {
                    authentication-none;
                    privacy-none;
                }
                user user4 {
                    authentication-md5 {
                        authentication-password authentication-password;
                    }
                    privacy-des {
                        privacy-password authentication-password;
                    }
                }
                user user5 {
                    authentication-sha {
                        authentication-password authentication-password;
                    }
                    privacy-aes128 {
                        privacy-password authentication-password;
                    }
                }
            }
```

```
    }
  }
}
```

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the SNMPv3 Authentication Type

IN THIS SECTION

- Configuring MD5 Authentication | 665
- Configuring SHA Authentication | 666
- Configuring No Authentication | 666

By default, in a Junos OS configuration the SNMPv3 authentication type is set to none.

This topic includes the following sections:

Configuring MD5 Authentication

To configure the message digest algorithm (MD5) as the authentication type for an SNMPv3 user, include the **authentication-md5** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-md5 {
  authentication-password authentication-password;
}
```

authentication-password is the password used to generate the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.

- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring SHA Authentication

To configure the secure hash algorithm (SHA) as the authentication type for an SNMPv3 user, include the **authentication-sha** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-sha {
    authentication-password authentication-password;
}
```

authentication-password is the password used to generate the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring No Authentication

To configure no authentication for an SNMPv3 user, include the **authentication-none** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-none;
```

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

Defining Access Privileges for an SNMP Group | 669

Configuring the Access Privileges Granted to a Group | 671

Assigning Security Model and Security Name to a Group | 676

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the SNMPv3 Encryption Type

IN THIS SECTION

- Configuring the Advanced Encryption Standard Algorithm | 667
- Configuring the Data Encryption Algorithm | 668
- Configuring Triple DES | 668
- Configuring No Encryption | 669

By default, encryption is set to none.

> **NOTE:** Before you configure encryption, you must configure MD5 or SHA authentication.
>
> Before you configure the **privacy-des**, **privacy-3des** and **privacy-aes128** statements, you must install the **jcrypto** package, and either restart the SNMP process or reboot the router.

This topic includes the following sections:

Configuring the Advanced Encryption Standard Algorithm

To configure the Advanced Encryption Standard (AES) algorithm for an SNMPv3 user, include the **privacy-aes128** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-aes128 {
    privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring the Data Encryption Algorithm

To configure the data encryption algorithm (DES) for an SNMPv3 user, include the **privacy-des** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-des {
    privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring Triple DES

To configure triple DES for an SNMPv3 user, include the **privacy-3des** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-3des {
    privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring No Encryption

To configure no encryption for an SNMPv3 user, include the **privacy-none** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-none;
```

RELATED DOCUMENTATION

- Configuring the SNMPv3 Authentication Type | 665
- Defining Access Privileges for an SNMP Group | 669
- Configuring the Access Privileges Granted to a Group | 671
- Assigning Security Model and Security Name to a Group | 676
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Defining Access Privileges for an SNMP Group

The SNMP version 3 (SNMPv3) uses the view-based access control model (VACM), which allows you to configure the access privileges granted to a group. Access is controlled by filtering the MIB objects available for a specific operation through a predefined view. You assign views to determine the objects that are visible for read, write, and notify operations for a particular group, using a particular context, a particular security model (v1, v2c, or usm), and particular security level (authenticated, privacy, or none). For information about how to configure views, see "Configuring MIB Views" on page 612.

You define user access to management information at the **[edit snmp v3 vacm]** hierarchy level. All access control within VACM operates on groups, which are collections of users as defined by USM, or community strings as defined in the SNMPv1 and SNMPv2c security models. The term ***security-name*** refers to these generic end users. The group to which a specific security name belongs is configured at the **[edit snmp v3 vacm security-to-group]** hierarchy level. That security name can be associated with a group defined at the **[edit snmp v3 vacm security-to-group]** hierarchy level. A group identifies a collection of SNMP users that share the same access policy. You then define the access privileges associated with a group at the **[edit snmp v3 vacm access]** hierarchy level. Access privileges are defined using views. For each group, you can apply different views depending on the SNMP operation; for example, read (**get**, **getNext**, or **getBulk**) write (**set**), notifications, the security level used (authentication, privacy, or none), and the security model (v1, v2c, or usm) used within an SNMP request.

You configure members of a group with the **security-name** statement. For v3 packets using USM, the security name is the same as the username. For SNMPv1 or SNMPv2c packets, the security name is

determined based on the community string. Security names are specific to a security model. If you are also configuring VACM access policies for SNMPv1 or SNMPv2c packets, you must assign security names to groups for each security model (SNMPv1 or SNMPv2c) at the **[edit snmp v3 vacm security-to-group]** hierarchy level. You must also associate a security name with an SNMP community at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

To configure the access privileges for an SNMP group, include statements at the **[edit snmp v3 vacm]** hierarchy level:

```
[edit snmp v3 vacm]
access {
    group group-name {
        (default-context-prefix | context-prefix context-prefix){
            security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                }
            }
        }
    }
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
```

RELATED DOCUMENTATION

- Configuring the SNMPv3 Authentication Type | 665
- Configuring the Access Privileges Granted to a Group | 671
- Assigning Security Model and Security Name to a Group | 676
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the Access Privileges Granted to a Group

IN THIS SECTION

- Configuring the Group | 671
- Configuring the Security Model | 671
- Configuring the Security Level | 672
- Associating MIB Views with an SNMP User Group | 672

This topic includes the following sections:

Configuring the Group

To configure the access privileges granted to a group, include the **group** statement at the **[edit snmp v3 vacm access]** hierarchy level:

```
[edit snmp v3 vacm access]
group group-name;
```

group-name is a collection of SNMP users that belong to a common SNMP list that defines an access policy. Users belonging to a particular SNMP group inherit all access privileges granted to that group.

Configuring the Security Model

To configure the security model, include the **security-model** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)]
security-model (any | usm | v1 | v2c);
```

- **any**—Any security model
- **usm**—SNMPv3 security model
- **v1**—SNMPV1 security model
- **v2c**—SNMPv2c security model

Configuring the Security Level

To configure the access privileges granted to packets with a particular security level, include the **security-level** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model (any | usm | v1 | v2c)]
security-level (authentication | none | privacy);
```

- **none**—Provides no authentication and no encryption.
- **authentication**—Provides authentication but no encryption.
- **privacy**—Provides authentication and encryption.

> **NOTE:** Access privileges are granted to all packets with a security level equal to or greater than that configured. If you are configuring the SNMPv1 or SNMPv2c security model, use **none** as your security level. If you are configuring the SNMPv3 security model (USM), use the **authentication**, **none**, or **privacy** security level.

SEE ALSO

- Configuring the SNMPv3 Authentication Type | 665
- Defining Access Privileges for an SNMP Group | 669
- Assigning Security Model and Security Name to a Group | 676
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Associating MIB Views with an SNMP User Group

IN THIS SECTION

- Configuring the Notify View | 673
- Configuring the Read View | 674
- Configuring the Write View | 674

MIB views define access privileges for members of a group. Separate views can be applied for each SNMP operation (read, write, and notify) within each security model (usm, v1, and v2c) and each security level (authentication, none, and privacy) supported by SNMP.

To associate MIB views with an SNMP user group, include the following statements at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level:

```
[edit snmp v3 vacm accessgroup group-name (default-context-prefix | context-prefix context-prefix)security-model
    (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
notify-view view-name;
read-view view-name;
write-view view-name;
```

> **NOTE:** You must associate at least one view (notify, read, or write) at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level.
>
> You must configure the MIB view at the **[edit snmp view *view-name*]** hierarchy level. For information about how to configure MIB views, see "Configuring MIB Views" on page 612.

This section describes the following topics related to this configuration:

Configuring the Notify View

To associate notify access with an SNMP user group, include the **notify-view** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model
    (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
notify-view view-name;
```

view-name specifies the notify access, which is a list of notifications that can be sent to each user in an SNMP group. A view name cannot exceed 32 characters.

Configuring the Read View

To associate a read view with an SNMP group, include the **read-view** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model
   (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
read-view view-name;
```

view-name specifies read access for an SNMP user group. A view name cannot exceed 32 characters.

Configuring the Write View

To associate a write view with an SNMP user group, include the **write-view** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model
   (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
write-view view-name;
```

view-name specifies write access for an SNMP user group. A view name cannot exceed 32 characters.

RELATED DOCUMENTATION

- Configuring the SNMPv3 Authentication Type | **665**
- Defining Access Privileges for an SNMP Group | **669**
- Assigning Security Model and Security Name to a Group | **676**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Example: Configuring the Access Privileges Granted to a Group | **674**

Example: Configuring the Access Privileges Granted to a Group

Define access privileges:

```
[edit snmp v3 vacm]
access {
   group group1 {
      default-context-prefix {
```

```
            security-model usm {          #Define an SNMPv3 security model
                security-level privacy {
                    notify-view nv1;
                    read-view rv1;
                    write-view wv1;
                }
            }
        }
        context-prefix lr1/ri1{ # routing instance ri1 in logical system lr1
            security-model usm {
                security-level privacy {
                    notify-view nv1;
                    read-view rv1;
                    write-view wv1;
                }
            }
        }
    }
    group group2 {
        default-context-prefix {
            security-model usm {          #Define an SNMPv3 security model
                security-level authentication {
                    read-view rv2;
                    write-view wv2;
                }
            }
        }
    }
    group group3 {
        default-context-prefix {
            security-model v1 {          #Define an SNMPv3 security model
                security-level none {
                    read-view rv3;
                    write-view wv3;
                }
            }
        }
    }
}
```

RELATED DOCUMENTATION

Configuring the Access Privileges Granted to a Group | 671

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Assigning Security Model and Security Name to a Group

IN THIS SECTION

- Configuring the Security Model | 676
- Assigning Security Names to Groups | 677
- Configuring the Group | 677

To assign security names to groups, include the following statements at the **[edit snmp v3 vacm security-to-group]** hierarchy level:

```
[edit snmp v3 vacm security-to-group]
security-model (usm | v1 | v2c) {
    security-name security-name {
        group group-name;
    }
}
```

This topic includes the following sections:

Configuring the Security Model

To configure the security model, include the **security-model** statement at the **[edit snmp v3 vacm security-to-group]** hierarchy level:

```
[edit snmp v3 vacm security-to-group]
security-model (usm | v1 | v2c);
```

- **usm**—SNMPv3 security model
- **v1**—SNMPv1 security model
- **v2c**—SNMPv2 security model

Assigning Security Names to Groups

To associate a security name with an SNMPv3 user, or a v1 or v2 community string, include the **security-name** statement at the **[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]** hierarchy level:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
security-name security-name;
```

For SNMPv3, the ***security-name*** is the username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level. For information about configuring usernames, see "Creating SNMPv3 Users" on page 662. For information about configuring a community string, see "Configuring the SNMPv3 Community" on page 703.

> **NOTE:** The USM security name is separate from the SNMPv1 and SNMPv2c security name. If you support SNMPv1 and SNMPv2c in addition to SNMPv3, you must configure separate security names within the security-to-group configuration at the **[edit snmp v3 vacm access]** hierarchy level.

Configuring the Group

After you have created SNMPv3 users, or v1 or v2 security names, you associate them with a group. A group is a set of security names belonging to a particular security model. A group defines the access rights for all users belonging to it. Access rights define what SNMP objects can be read, written to, or created. A group also defines what notifications a user is allowed to receive.

If you already have a group that is configured with all of the view and access permissions that you want to give a user, you can add the user to that group. If you want to give a user view and access permissions that no other groups have, or if you do not have any groups configured, create a group and add the user to it.

To configure the access privileges granted to a group, include the **group** statement at the **[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name *security-name*]** hierarchy level:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name security-name]
group group-name;
```

group-name identifies a collection of SNMP security names that share the same access policy. For more information about groups, see "Defining Access Privileges for an SNMP Group" on page 669.

SEE ALSO

Configuring the SNMPv3 Authentication Type | 665
Defining Access Privileges for an SNMP Group | 669
Configuring the Access Privileges Granted to a Group | 671
Minimum SNMPv3 Configuration on a Device Running Junos OS | 657
Example: Security Group Configuration | 678

Example: Security Group Configuration

Assign security names to groups:

```
vacm {
    security-to-group {
        security-model usm {
            security-name user1 {
                group group1;
            }
            security-name user2 {
                group group2;
            }
            security-name user3 {
                group group3;
            }
        }
    }
}
```

RELATED DOCUMENTATION

Assigning Security Model and Security Name to a Group | 676
Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring SNMPv3 Traps on a Device Running Junos OS

In SNMPv3, you create traps and informs by configuring the **notify**, **target-address**, and **target-parameters** parameters. Traps are unconfirmed notifications, whereas informs are confirmed notifications. This section

describes how to configure SNMP traps. For information about configuring SNMP informs, see "Configuring SNMP Informs" on page 692.

The target address defines a management application's address and parameters to be used in sending notifications. Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target. SNMPv3 also lets you define SNMPv1 and SNMPv2c traps.

> **NOTE:** When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Access privileges are configured at the **[edit snmp v3 vacm access]** and **[edit snmp v3 vacm security-to-group]** hierarchy levels.

To configure SNMP traps, include the following statements at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify name {
    tag tag-name;
    type trap;
}
notify-filter name {
    oid object-identifier (include | exclude);
}
target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
```

RELATED DOCUMENTATION

Configuring the SNMPv3 Trap Notification | 680
Configuring the Trap Notification Filter | 682
Configuring the Trap Target Address | 683
Defining and Configuring the Trap Target Parameters | 688
Configuring SNMP Informs | 692
Configuring the Remote Engine and Remote User | 696
Configuring the Inform Notification Type and Target Address | 693

Configuring the SNMPv3 Trap Notification

The **notify** statement specifies the type of notification (trap) and contains a single tag. The tag defines a set of target addresses to receive a trap. The tag list contains one or more tags and is configured at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level. If the tag list contains this tag, Junos OS sends a notification to all the target addresses associated with this tag.

To configure the trap notifications, include the **notify** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify name {
    tag tag-name;
    type trap;
}
```

name is the name assigned to the notification.

tag-name defines the target addresses to which this notification is sent. This notification is sent to all the target-addresses that have this tag in their tag list. The ***tag-name*** is not included in the notification.

trap is the type of notification.

> **NOTE:** Each notify entry name must be unique.
>
> Junos OS supports two types of notification: **trap** and **inform**.

For information about how to configure the tag list, see "Configuring the Trap Target Address" on page 685.

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | 678
- Configuring the Trap Notification Filter | 682
- Configuring the Trap Target Address | 683
- Defining and Configuring the Trap Target Parameters | 688
- Configuring SNMP Informs | 692
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Example: Configuring SNMPv3 Trap Notification

Specify three sets of destinations to send traps:

```
[edit snmp v3]
notify n1 {
    tag router1;
    type trap;
}
notify n2 {
    tag router2;
    type trap
}
notify n3 {
    tag router3;
    type trap;
}
```

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | 678
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the Trap Notification Filter

SNMPv3 uses the notify filter to define which traps (or which objects from which traps) are sent to the network management system (NMS). The trap notification filter limits the type of traps that are sent to the NMS.

Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as 1.3.6.1.2.1.2) or by its subtree name (such as **interfaces**). You can also use the wildcard character asterisk (*) in the object identifier (OID) to specify object identifiers that match a particular pattern.

To configure the trap notifications filter, include the **notify-filter** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify-filter profile-name;
```

profile-name is the name assigned to the notify filter.

By default, the OID is set to **include**. To define access to traps (or objects from traps), include the **oid** statement at the **[edit snmp v3 notify-filter *profile-name*]** hierarchy level:

```
[edit snmp v3 notify-filter profile-name]
oid oid (include | exclude);
```

oid is the object identifier. All MIB objects represented by this statement have the specified OID as a prefix. It can be specified either by a sequence of dotted integers or by a subtree name.

- **include**—Include the subtree of MIB objects represented by the specified OID.
- **exclude**—Exclude the subtree of MIB objects represented by the specified OID.

RELATED DOCUMENTATION

Configuring SNMPv3 Traps on a Device Running Junos OS | 678

Configuring the SNMPv3 Trap Notification | 680

Configuring the Trap Target Address | 683

Defining and Configuring the Trap Target Parameters | 688

Configuring SNMP Informs | 692

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the Trap Target Address

IN THIS SECTION

- Configuring the Address | 684
- Configuring the Address Mask | 684
- Configuring the Port | 685
- Configuring the Routing Instance | 685
- Configuring the Trap Target Address | 685
- Applying Target Parameters | 686

The target address defines a management application's address and parameters that are used in sending notifications. It can also identify management stations that are allowed to use specific community strings. When you receive a packet with a recognized community string and a tag is associated with it, Junos OS looks up all the target addresses with this tag and verifies that the source address of this packet matches one of the configured target addresses.

NOTE: You must configure the address mask when you configure the SNMP community.

To specify where you want the traps to be sent and define what SNMPv1 and SNMPv2cc packets are allowed, include the **target-address** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
target-address target-address-name;
```

target-address-name is the string that identifies the target address.

To configure the target address properties, include the following statements at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
address address;
address-mask address-mask;
logical-system logical-system;
port port-number;
```

```
routing-instance instance;
tag-list tag-list;
target-parameters target-parameters-name;
```

Unlike with SNMP v2, In SNMPv3, there is no configuration option to limit inbound polling. But you can configure a lo0 filter to limit inbound polling by creating a rule to allow SNMP from your monitoring system IPs. For example:

```
set policy-options prefix-list SNMP 10.1.1.1/32
set policy-options prefix-list SNMP 192.168.1.0/24

set firewall family inet filter CoPP term SNMP from source-prefix-list SNMP
set firewall family inet filter CoPP term SNMP from protocol udp
set firewall family inet filter CoPP term SNMP from destination-port snmp
set firewall family inet filter CoPP term SNMP then accept
set firewall family inet filter CoPP term SNMP then count SNMP
```

Configuring the Address

To configure the address, include the **address** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
address address;
```

address is the SNMP target address.

Configuring the Address Mask

The address mask specifies a set of addresses that are allowed to use a community string and verifies the source addresses for a group of target addresses.

To configure the address mask, include the **address-mask** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
address-mask address-mask;
```

address-mask combined with the address defines a range of addresses. For information about how to configure the community string, see “Configuring the SNMPv3 Community” on page 703.

Configuring the Port

By default, the UDP port is set to 162. To configure a different port number, include the **port** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
port port-number;
```

port-number is the SNMP target port number.

Configuring the Routing Instance

Traps are sent over the default routing instance. To configure the routing instance for sending traps, include the **routing-instance** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
routing-instance instance;
```

instance is the name of the routing instance. To configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (**/**) to separate the two names (for example, **test-lr/test-ri**). To configure the default routing instance on a logical system, specify the logical system name followed by **default** (for example, **test-lr/default**).

Configuring the Trap Target Address

Each **target-address** statement can have one or more tags configured in its tag list. Each tag can appear in more than one tag list. When a significant event occurs on the network device, the tag list identifies the targets to which a notification is sent.

To configure the tag list, include the **tag-list** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
tag-list "tag-list";
```

tag-list specifies one or more tags as a space-separated list enclosed within double quotes.

For an example of tag list configuration, see "Example: Configuring the Tag List" on page 687.

For information about how to specify a tag at the **[edit snmp v3 notify *notify-name*]** hierarchy level, see "Configuring the SNMPv3 Trap Notification" on page 680.

NOTE: When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Configure access privileges at the **[edit snmp v3 vacm access]** hierarchy level.

Applying Target Parameters

The **target-parameters** statement at the **[edit snmp v3]** hierarchy level applies the target parameters configured at the **[edit snmp v3 target-parameters *target-parameters-name*]** hierarchy level.

To reference configured target parameters, include the **target-parameters** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
target-parameters target-parameters-name;
```

target-parameters-name is the name associated with the message processing and security parameters that are used in sending notifications to a particular management target.

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | **678**
- Configuring the SNMPv3 Trap Notification | **680**
- Configuring the Trap Notification Filter | **682**
- Defining and Configuring the Trap Target Parameters | **688**
- Configuring SNMP Informs | **692**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Example: Configuring the Tag List | **687**

Example: Configuring the Tag List

In the following example, two tag entries (**router1** and **router2**) are defined at the **[edit snmp v3 notify *notify-name*]** hierarchy level. When an event triggers a notification, Junos OS sends a trap to all target addresses that have **router1** or **router2** configured in their target-address tag list. This results in the first two targets getting one trap each, and the third target getting two traps.

```
[edit snmp v3]
notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap; # Defines the type of notification
}
notify n2 {
    tag router2;
    type trap;
}
target-address ta1 {
    address 10.1.1.1;
    address-mask 255.255.255.0;
    port 162;
    tag-list router1;
    target-parameters tp1;
}
target-address ta2 {
    address 10.1.1.2;
    address-mask 255.255.255.0;
    port 162;
    tag-list router2;
    target-parameters tp2;
}
target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list “router1 router2”; #Define multiple tags in the target address tag list
    target-parameters tp3;
}
```

RELATED DOCUMENTATION

Configuring SNMPv3 Traps on a Device Running Junos OS | 678

Configuring the Trap Target Address | 683

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Defining and Configuring the Trap Target Parameters

IN THIS SECTION

- Applying the Trap Notification Filter | 689
- Configuring the Target Parameters | 689

Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target.

To define a set of target parameters, include the **target-parameters** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
target-parameters target-parameters-name;
```

target-parameters-name is the name assigned to the target parameters.

To configure target parameter properties, include the following statements at the **[edit snmp v3 target-parameters *target-parameter-name*]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name]
notify-filter profile-name;
parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
}
```

NOTE: When you configure SNMP trap notifications for subscriber secure policy on MX Series routers, you must configure the parameters as follows:

- Message-processing model: **v3**
- Security level: **privacy**
- Security model: **usm**

For more information about configuring subscriber secure policies, see *Subscriber Secure Policy Overview*.

This topic includes the following sections:

Applying the Trap Notification Filter

To apply the trap notification filter, include the **notify-filter** statement at the **[edit snmp v3 target-parameters *target-parameter-name*]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name]
notify-filter profile-name;
```

profile-name is the name of a configured notify filter. For information about configuring notify filters, see "Configuring the Trap Notification Filter" on page 682.

Configuring the Target Parameters

IN THIS SECTION

- Configuring the Message Processing Model | **690**
- Configuring the Security Model | **690**
- Configuring the Security Level | **691**
- Configuring the Security Name | **691**

To configure target parameter properties, include the following statements at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
message-processing-model (v1 | v2c | v3);
security-level (authentication | none | privacy);
security-model (usm | v1 | v2c);
security-name security-name;
```

This section includes the following topics:

Configuring the Message Processing Model

The message processing model defines which version of SNMP to use when generating SNMP notifications. To configure the message processing model, include the **message-processing-model** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
message-processing-model (v1 | v2c | v3);
```

- **v1**—SNMPv1 message processing model
- **v2c**—SNMPv2c message processing model
- **v3**—SNMPV3 message processing model

> **NOTE:** The **v3** message-processing model is required for subscriber secure policy on MX Series routers. See *Subscriber Secure Policy Overview* for more information.

Configuring the Security Model

To define the security model to use when generating SNMP notifications, include the **security-model** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
security-model (usm | v1 | v2c);
```

- **usm**—SNMPv3 security model
- **v1**—SNMPv1 security model
- **v2c**—SNMPv2c security model

> **NOTE:** The **usm** security model is required for subscriber secure policy on MX Series routers. See *Subscriber Secure Policy Overview* for more information.

Configuring the Security Level

The **security-level** statement specifies whether the trap is authenticated and encrypted before it is sent.

To configure the security level to use when generating SNMP notifications, include the **security-level** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
security-level (authentication | none | privacy);
```

- **authentication**—Provides authentication but no encryption.
- **none**—No security. Provides no authentication and no encryption.
- **privacy**—Provides authentication and encryption.

> **NOTE:** If you are configuring the SNMPv1 or SNMPV2c security model, use **none** as your security level. If you are configuring the SNMPv3 (USM) security model, use the **authentication** or **privacy** security level.
>
> The **privacy** security level is required for subscriber secure policy on MX Series routers. See *Subscriber Secure Policy Overview* for more information.

Configuring the Security Name

To configure the security name to use when generating SNMP notifications, include the **security-name** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
security-name security-name;
```

If the USM security model is used, the **security-name** identifies the user that is used when the notification is generated. If the v1 or v2c security models are used, **security-name** identifies the SNMP community used when the notification is generated.

NOTE: The access privileges for the group associated with a security name must allow this notification to be sent.

If you are using the v1 or v2 security models, the security name at the **[edit snmp v3 vacm security-to-group]** hierarchy level must match the security name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | **678**
- Configuring the SNMPv3 Trap Notification | **680**
- Configuring the Trap Notification Filter | **682**
- Configuring the Trap Target Address | **683**
- Configuring SNMP Informs | **692**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

Configuring SNMP Informs

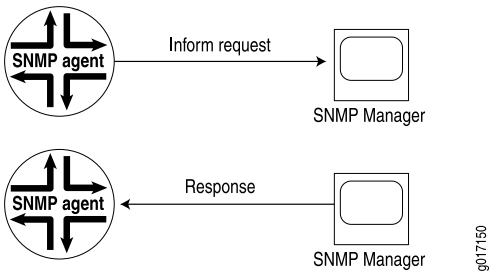
Junos OS supports two types of notifications: traps and informs. With traps, the receiver does not send any acknowledgment when it receives a trap. Therefore, the sender cannot determine if the trap was received. A trap may be lost because a problem occurred during transmission. To increase reliability, an inform is similar to a trap except that the inform is stored and retransmitted at regular intervals until one of these conditions occurs:

- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted and the agent discards the inform message.

If the sender never receives a response, the inform can be sent again. Thus, informs are more likely to reach their intended destination than traps are. Informs use the same communications channel as traps (same socket and port) but have different protocol data unit (PDU) types.

Informs are more reliable than traps, but they consume more network, router, and switch resources (see Figure 26 on page 693). Unlike a trap, an inform is held in memory until a response is received or the timeout is reached. Also, traps are sent only once, whereas an inform may be retried several times. Use informs when it is important that the SNMP manager receive all notifications. However, if you are more concerned about network traffic, or router and switch memory, use traps.

Figure 26: Inform Request and Response



For information about configuring SNMP traps, see "Configuring SNMPv3 Traps on a Device Running Junos OS" on page 678.

RELATED DOCUMENTATION

Configuring SNMPv3 Traps on a Device Running Junos OS | 678

Configuring the Remote Engine and Remote User | 696

Configuring the Inform Notification Type and Target Address | 693

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the Inform Notification Type and Target Address

To configure the inform notification type and target information, include the following statements at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify name {
    tag tag-name;
    type (trap | inform);
}
target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    retry-count number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
```

```
}
target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
```

notify *name* is the name assigned to the notification. Each notify entry name must be unique.

tag *tag-name* defines the target addresses that are sent this notification. The notification is sent to all target addresses that have this tag in their tag list. The ***tag-name*** is not included in the notification. For information about how to configure the tag list, see "Configuring the Trap Target Address" on page 685.

type inform is the type of notification.

target-address *target-address-name* identifies the target address. The target address defines a management application's address and parameters that are used to respond to informs.

timeout *seconds* is the number of seconds to wait for an acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted. The default timeout is **15** seconds.

retry-count *number* is the maximum number of times an inform is transmitted if no acknowledgment is received. The default is **3**. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.

message-processing-model defines which version of SNMP to use when SNMP notifications are generated. Informs require a **v3** message processing model.

security-model defines the security model to use when SNMP notifications are generated. Informs require a **usm** security model.

security-model defines the security model to use when SNMP notifications are generated. Informs require a **usm** security model.

security-level specifies whether the inform is authenticated and encrypted before it is sent. For the **usm** security model, the security level must be one of the following:

- **authentication**—Provides authentication but no encryption.
- **privacy**—Provides authentication and encryption.

security-name identifies the username that is used when generating the inform.

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | 678
- Configuring SNMP Informs | 692
- Configuring the Remote Engine and Remote User | 696
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657
- Example: Configuring the Inform Notification Type and Target Address | 695

Example: Configuring the Inform Notification Type and Target Address

In the following example, target 172.17.20.184 is configured to respond to informs. The inform timeout is 30 seconds and the maximum retransmit count is 3. The inform is sent to all targets in the tl1 list. The security model for the remote user is usm and the remote engine username is u10.

```
[edit snmp v3]
notify n1 {
    type inform;
    tag tl1;
}
notify-filter nf1 {
    oid .1.3 include;
}
target-address ta1 {
    address 172.17.20.184;
    retry-count 3;
    tag-list tl1;
    address-mask 255.255.255.0;
    target-parameters tp1;
    timeout 30;
}
target-parameters tp1 {
    parameters {
        message-processing-model v3;
        security-model usm;
        security-level privacy;
        security-name u10;
    }
    notify-filter nf1;
}
```

RELATED DOCUMENTATION

Configuring the Inform Notification Type and Target Address | 693

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Configuring the Remote Engine and Remote User

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. When sending an inform message, the agent uses the credentials of the user configured on the remote engine (inform target).

To configure a remote engine and remote user to receive and respond to SNMP informs, include the following statements at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
usm {
    remote-engine engine-id {
        user username {
            authentication-md5 {
                authentication-key key;
            }
            authentication-none;
            authentication-sha {
                authentication-key key;
            }
            privacy-3des {
                privacy-key key;
            }
            privacy-aes128 {
                privacy-key key;
            }
            privacy-des {
                privacy-key key;
            }
            privacy-none;
        }
    }
}
```

For informs, **remote-engine *engine-id*** is the identifier for the SNMP agent on the remote device where the user resides.

For informs, **user *username*** is the user on a remote SNMP engine who receives the informs.

Informs generated can be **unauthenticated**, **authenticated**, or **authenticated_and_encrypted**, depending on the security level of the SNMPv3 user configured on the remote engine (the inform receiver). The authentication key is used for generating message authentication code (MAC). The privacy key is used to encrypt the inform PDU part of the message.

RELATED DOCUMENTATION

- Configuring SNMPv3 Traps on a Device Running Junos OS | **678**
- Configuring SNMP Informs | **692**
- Configuring the Inform Notification Type and Target Address | **693**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Example: Configuring the Remote Engine ID and Remote User | **697**

Example: Configuring the Remote Engine ID and Remote User

IN THIS SECTION

- Requirements | **698**
- Overview | **698**
- Configuration | **699**
- Verification | **700**

This example shows how to configure a remote engine and remote user so you can receive and respond to SNMP inform notifications. Inform notifications can be authenticated and encrypted. They are also more reliable than traps, another type of notification that Junos OS supports. Unlike traps, inform notifications are stored and retransmitted at regular intervals until one of these conditions occurs:

- The target of the inform notification returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted.

Requirements

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

This feature requires the use of plain-text passwords valid for SNMPv3. SNMPv3 has the following special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Although quotation marks are not always required to enclose passwords, it is best to use them. You need quotation marks if the password contains any spaces or possibly in the case of certain special characters or punctuation.

Overview

Inform notifications are supported in SNMPv3 to increase reliability. For example, an SNMP agent receiving an inform notification acknowledges the receipt.

For inform notifications, the remote engine ID identifies the SNMP agent on the remote device where the user resides, and the username identifies the user on a remote SNMP engine who receives the inform notifications.

Consider a scenario in which you have the values in Table 50 on page 698 to use in configuring the remote engine ID and remote user in this example.

Table 50: Values to Use in Example

Name of Variable	Value
username	u10
remote engine ID	800007E5804089071BC6D10A41
authentication type	authentication-md5
authentication password	qol67R%?
encryption type	privacy-des
privacy password	m*72Jl9v

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste these commands into the CLI at the **[edit snmp v3]** hierarchy level, and then enter **commit** from configuration mode.

```
set usm remote-engine 800007E5804089071BC6D10A41 user u10 authentication-md5 authentication-key
    "qol67R%?"
set usm remote-engine 800007E5804089071BC6D10A41 user u10 privacy-des privacy-key "m*72Jl9v"
```

Configuring the Remote Engine and Remote User

Step-by-Step Procedure

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

To configure the remote engine ID and remote user:

1. Configure the remote engine ID, username, and authentication type and password.

   ```
   [edit snmp v3]
   user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10 authentication-md5
       authentication-key "qol67R%?"
   ```

2. Configure the encryption type and privacy password.

   You can configure only one encryption type per SNMPv3 user.

   ```
   [edit snmp v3]
   user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10 privacy-des privacy-key
       "m*72Jl9v"
   ```

Results

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

```
[edit snmp v3]
user@ host# show
```

```
usm {
    remote-engine 800007E5804089071BC6D10A41 {
        user u10 {
            authentication-md5 {
                authentication-key "$9$Tz/teK8NdsLXk.f5n6p0ORev"; ## SECRET-DATA
            }
            privacy-des {
                privacy-key "$9$/gyNCu1KvWdwYMWw2gJHkRhcrWx"; ## SECRET-DATA
            }
        }
    }
}
```

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

Verification

Verifying the Configuration of the Remote Engine ID and Username

Purpose

Verify the status of the engine ID and user information.

Action

Display information about the SNMPv3 engine ID and user.

`user@host>` **show snmp v3**

```
Local engine ID: 80 00 0a 4c 01 0a ff 03 e3
Engine boots:           3
Engine time:       769187 seconds
Max msg size:       65507 bytes

Engine ID: 80 00 07 e5 80 40 89 07 1b c6 d1 0a 41
    User                            Auth/Priv   Storage      Status
    u10                              md5/des    nonvolatile  active
```

Meaning

The output displays the following information:

- Local engine ID and detail about the engine
- Remote engine ID (labeled **Engine ID**)
- Username

- Authentication type and encryption (privacy) type that is configured for the user
- Type of storage for the username, either nonvolatile (configuration saved) or volatile (not saved)
- Status of the new user; only users with an active status can use SNMPv3

RELATED DOCUMENTATION

show snmp v3 | 2912

Configuring the SNMPv3 Encryption Type | 667

Configuring the SNMPv3 Authentication Type | 665

Configuring SNMP Informs | 692

Configuring the Remote Engine and Remote User | 696

Configuring the Local Engine ID

By default, the local engine ID uses the default IP address of the router. The local engine ID is the administratively unique identifier for the SNMPv3 engine. This statement is optional. To configure the local engine ID, include the **engine-id** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
engine-id {
    (local engine-id-suffix | use-default-ip-address | use-mac-address);
}
```

- **local *engine-id-suffix***—The engine ID suffix is explicitly configured.
- **use-default-ip-address**—The engine ID suffix is generated from the default IP address.
- **use-mac-address**—The SNMP engine identifier is generated from the Media Access Control (MAC) address of the management interface on the router.

NOTE: If you are using SNMPv3 and if the engine ID is based on the MAC address and you upgrade from an earlier release to one of these releases (14.1X53-D50, 16.1R5, 17.1R2, 17.2R1, 15.1X53-D231, 14.1X53-D43, 15.1X53-D232), you must reconfigure SNMPv3 because the engine ID is changed by the upgrade. If you do not reconfigure SNMPv3, you will see authentication error for SNMPv3 polling because the engine ID is changed after the upgrade. You only need to reconfigure SNMPv3 on the first such upgrade. If you then upgrade from one of the mentioned releases to another of these releases, you do not have to upgrade SNMPv3 again.

To reconfigure SNMPv3, use the following procedure. Do not use the **rollback 1** command.

To reconfigure SNMPv3:

1. Check what the SNMPv3 configuration is.

```
user@host# show snmp v3
```

2. Delete the SNMPv3 configuration.

```
user@host# delete snmp v3
```

3. Reconfigure SNMPv3 configuration (see ouput from Step 1).

The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*. You can configure the suffix here.

NOTE: SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise, the keys generated from the configured passwords are based on the previous engine ID. For the engine ID, we recommend using the master IP address of the device if the device has multiple routing engines and has the master IP address configured. Alternatively, you can use the MAC address of the management port if the device has only one Routing Engine.

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

Example: SNMPv3 Configuration | 658

Configuring the SNMPv3 Community

IN THIS SECTION

- Configuring the Community Name | 704
- Configuring the Context | 704
- Configuring the Security Names | 705
- Configuring the Tag | 705

The SNMP community defines the relationship between an SNMP server system and the client systems. This statement is optional.

To configure the SNMP community, include the **snmp-community** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
snmp-community community-index;
```

community-index is the index for the SNMP community.

To configure the SNMP community properties, include the following statements at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
community-name community-name;
context context-name;
security-name security-name;
tag tag-name;
```

This section includes the following topics:

Configuring the Community Name

The community name defines the SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2c clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (read, write, or notify) allowed on those objects.

To configure the SNMP community name, include the **community-name** statement at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
community-name community-name;
```

community-name is the community string for an SNMPv1 or SNMPv2c community.

If unconfigured, it is the same as the community index.

If the community name contains spaces, enclose it in quotation marks (“ “).

> **NOTE:** Community names must be unique. You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community *community-index*]** hierarchy levels. The configured community name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level is encrypted. You cannot view the community name after you have configured it and committed your changes. In the command-line interface (CLI), the community name is concealed.

Configuring the Context

An SNMP context defines a collection of management information that is accessible to an SNMP entity. Typically, an SNMP entity has access to multiple contexts. A context can be a physical or logical system, a collection of multiple systems, or even a subset of a system. Each context in a management domain has a unique identifier.

To configure an SNMP context, include the **context *context-name*** statement at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
context context-name;
```

> **NOTE:** To query a routing instance or a logical system,

Configuring the Security Names

To assign a community string to a security name, include the **security-name** statement at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
security-name security-name;
```

security-name is used when access control is set up. The **security-to-group** configuration at the **[edit snmp v3 vacm]** hierarchy level identifies the group.

> **NOTE:** This security name must match the security name configured at the **[edit snmp v3 target-parameters *target-parameters-name* parameters]** hierarchy level when you configure traps.

Configuring the Tag

To configure the tag, include the **tag** statement at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
tag tag-name;
```

tag-name identifies the address of managers that are allowed to use a community string.

RELATED DOCUMENTATION

- Creating SNMPv3 Users | 662
- Minimum SNMPv3 Configuration on a Device Running Junos OS | 657
- Example: Configuring an SNMPv3 Community | 706

Example: Configuring an SNMPv3 Community

IN THIS SECTION

- Requirements | 706
- Overview | 706
- Configuration | 706
- Verification | 709

This example shows how to configure an SNMPv3 community.

Requirements

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

Overview

This example demonstrates how to create an SNMPv3 community. Define the SNMP community name, specify security name to perform the access control, and define tag name which identifies the address of managers that are allowed to use a community string. The target address defines a management application's address and parameters that are used in sending notifications.

When the device receives a packet with a recognized community string and a tag is associated with that packet, the Junos software looks up all the target addresses with this tag and verifies that the source address of this packet matches one of the configured target addresses.

Specify where you want the traps to be sent and define what SNMPv1 and SNMPv2c packets are allowed. Specify target address name that identifies the target address, define the target address, mask range of address, port number, tag list, and target parameter.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit snmp v3]** hierarchy level, and then enter **commit** from configuration mode.

```
set snmp-community index1 community-name "public"
set snmp-community index1 security-name john
set snmp-community index1 tag router1
set target-address ta1 address 10.1.1.1
set target-address ta1 address-mask 255.255.255.0
set target-address ta1 port 162
set target-address ta1 tag-list router1
set target-address ta1 target-parameters tp1
```

Step-by-Step Procedure

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

1. Configure the SNMP community name.

   ```
   [edit snmp v3]
   user@host# set snmp-community index1 community-name "public"
   ```

   NOTE: The SNMP community name must be unique.

2. Configure the security name to perform access control.

   ```
   [edit snmp v3]
   user@host# set snmp-community index1 security-name john
   ```

3. Define the tag name. The tag name identifies the address of managers that are allowed to use a community string.

   ```
   [edit snmp v3]
   user@host# set snmp-community index1 tag router1
   ```

4. Configure SNMP target address.

   ```
   [edit snmp v3]
   user@host# set target-address ta1 address 10.1.1.1
   ```

5. Configure the mask range of the address for the community string access control.

```
[edit snmp v3]
user@host#set target-address ta1 address-mask 255.255.255.0
```

6. Configure SNMPv3 target port number.

```
[edit snmp v3]
user@host#set target-address ta1 port 162
```

7. Configure SNMPv3 tag list to select the target addresses.

```
[edit snmp v3]
user@host#set target-address ta1 tag-list router1
```

8. Configure SNMPv3 target parameter name in the target parameter table.

```
[edit snmp v3]
user@host#set target-address ta1 target-parameters tp1
```

Results

From configuration mode, confirm your configuration by entering the **show snmp v3** command. If the output does not display the intended configuration, repeat the configuration instructions in this example.

```
[edit]
user@host# show snmp v3
target-address ta1 {
    address 10.1.1.1;
    port 162;
    tag-list router1;
    address-mask 255.255.255.0;
    target-parameters tp1;
}
snmp-community index1 {
    community-name "$9$JOZi.QF/AtOz3"; ## SECRET-DATA
    security-name john;
    tag router1;
}
```

Verification

Verifying SNMPv3 community

Purpose

Verify if SNMPv3 community is enabled.

Action

To verify SNMPv3 community configuration, enter **show snmp v3 community** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
Community           Security  Context  Tag          Storage      Status
index1              john               router1      nonvolatile  active
```

Meaning

The output displays the information about SNMPv3 community being enabled on the system.

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | **703**

Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

CHAPTER 16

Configuring SNMP for Routing Instances

IN THIS CHAPTER

- Understanding SNMP Support for Routing Instances | 710
- SNMPv3 Management Routing Instance | 712
- SNMP MIBs Supported for Routing Instances | 713
- Support Classes for MIB Objects | 725
- SNMP Traps Supported for Routing Instances | 726
- Identifying a Routing Instance | 726
- Enabling SNMP Access over Routing Instances | 727
- Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728
- Example: Configuring Interface Settings for a Routing Instance | 729
- Configuring Access Lists for SNMP Access over Routing Instances | 731
- SNMPv3 Management Routing Instance | 732

Understanding SNMP Support for Routing Instances

Junos OS enables SNMP managers for all routing instances to request and manage SNMP data related to the corresponding routing instances and logical system networks.

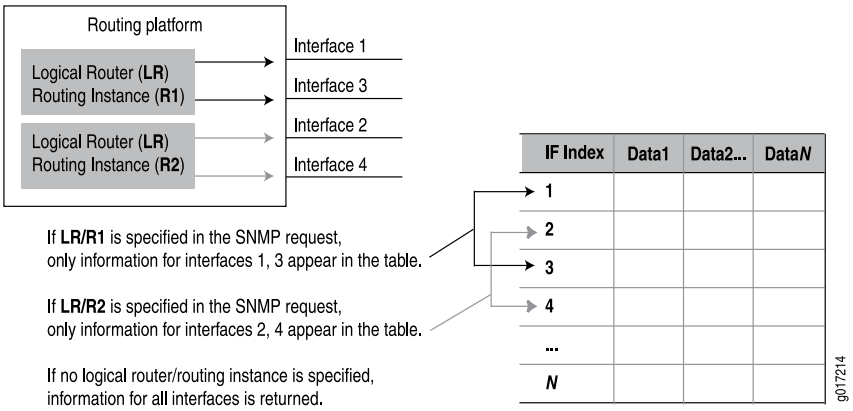
In Junos OS:

- Clients from routing instances other than the default can access MIB objects and perform SNMP operations only on the logical system networks to which they belong.
- Clients from the default routing instance can access information related to all routing instances and logical system networks.
- The Junos management routing instance (**mgmt_junos**) is a special instance. Clients from the management routing instance are treated as if they were in the default routing instance and can access information related to all routing instances and logical system networks.

Before Junos OS Release 8.4, only the SNMP manager in the default routing instance (inet.0) had access to the MIB objects.

With the increase in virtual private network (VPN) service offerings, this feature is useful particularly for service providers who need to obtain SNMP data for specific routing instances (see Figure 27 on page 711). Service providers can use this information for their own management needs or export the data for use by their customers.

Figure 27: SNMP Data for Routing Instances



If no routing instance is specified in the request, the SNMP agent operates as before:

- For nonrouting table objects, all instances are exposed.
- For routing table objects, only those associated with the default routing instance are exposed.

> **NOTE:** The actual protocol data units (PDUs) are still exchanged over the default (inet.0) routing instance, but the data contents returned are dictated by the routing instance specified in the request PDUs.

RELATED DOCUMENTATION

Support Classes for MIB Objects | **725**

SNMP Traps Supported for Routing Instances | **726**

Identifying a Routing Instance | **726**

Enabling SNMP Access over Routing Instances | **727**

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | **728**

Configuring Access Lists for SNMP Access over Routing Instances | **731**

SNMPv3 Management Routing Instance

Starting in Junos OS 19.4R1, you can access information related to all routing instances and logical system networks and not specific to ingress routing instance by configuring the SNMPv3 management interface in a required management instance. You can configure the management instance configuration statement at the **[edit SNMP v3]** hierarchy level.

Benefits

SNMPv3 management routing instance enables all the SNMPv3 requests from non-default routing instance as if the requests are from default routing instance. Using SNMPv3 management routing instance, you access the information related to all routing instances and logical system networks.

Enabling the Management Routing Instance

To enable the SNMPv3 management routing instance:

1. Configure the management-instance statement.

   [edit]
   `user@host#` **set SNMP v3 management-routing-instance <routing-instance>**

2. Commit the configuration.

   [edit]
   `user@host#` **commit**

Removing the Management Routing Instance

To remove the SNMPv3 management routing instance:

1. Delete or deactivate the SNMPv3 management routing instance statement.

   [edit]
   `user@host#` **delete SNMP v3 management-routing-instance <routing-instance>**

RELATED DOCUMENTATION

Understanding SNMP Support for Routing Instances | 710

SNMP MIBs Supported for Routing Instances

Table 51 on page 713 shows enterprise-specific MIB objects supported by Junos OS and provides notes detailing how they are handled when a routing instance is specified in an SNMP request. An en dash (–) indicates that the item is not applicable.

Table 51: MIB Support for Routing Instances (Juniper Networks MIBs)

Object	Support Class	Description/Notes
jnxProducts(1)	–	Product Object IDs
jnxServices(2)	–	Services
jnxMibs(3) jnxBoxAnatomy(1)	Class 3	Objects are exposed only for the default logical system.
mpls(2)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
ifJnx(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAlarms(4)	Class 3	Objects are exposed only for the default logical system.
jnxFirewalls(5)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxDCUs(6)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxPingMIB(7)	Class 3	Objects are exposed only for the default logical system.
jnxTraceRouteMIB(8)	Class 3	Objects are exposed only for the default logical system.

Table 51: MIB Support for Routing Instances (Juniper Networks MIBs) *(continued)*

Object	Support Class	Description/Notes
jnxATM(10)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxIpv6(11)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxIpv4(12)	Class 1	jnxIpv4AddrTable(1). Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxRmon(13)	Class 3	jnxRmonAlarmTable(1). Objects are exposed only for the default logical system.
jnxLdp(14)	Class 2	jnxLdpTrapVars(1). All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
jnxCos(15) jnxCosIfqStatsTable(1) jnxCosFcTable(2) jnxCosFcIdTable(3) jnxCosQstatTable(4)	Class 3	Objects are exposed only for the default logical system.
jnxScu(16) jnxScuStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxRpf(17) jnxRpfStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxCfgMgmt(18)	Class 3	Objects are exposed only for the default logical system.

Table 51: MIB Support for Routing Instances (Juniper Networks MIBs) *(continued)*

Object	Support Class	Description/Notes
jnxPMon(19) jnxPMonFlowTable(1) jnxPMonErrorTable(2) jnxPMonMemoryTable(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxSonet(20) jnxSonetAlarmTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAtmCos(21) jnxCosAtmVcTable(1) jnxCosAtmScTable(2) jnxCosAtmVcQstatsTable(3) jnxCosAtmTrunkTable(4)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
ipSecFlowMonitorMIB(22)	–	–
jnxMac(23) jnxMacStats(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
apsMIB(24)	Class 3	Objects are exposed only for the default logical system.
jnxChassisDefines(25)	Class 3	Objects are exposed only for the default logical system.
jnxVpnMIB(26)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
jnxSericesInfoMib(27)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.

Table 51: MIB Support for Routing Instances (Juniper Networks MIBs) *(continued)*

Object	Support Class	Description/Notes
jnxCollectorMIB(28)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxHistory(29)	–	–
jnxSpMIB(32)	Class 3	Objects are exposed only for the default logical system.

Table 52 on page 717 shows Class 1 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 1 objects, only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.

Table 52: Class 1 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 1	802.3ad.mib	(dot3adAgg) MIB objects: dot3adAggTable dot3adAggPortListTable (dot3adAggPort) dot3adAggPortTable dot3adAggPortStatsTable dot3adAggPortDebugTable
	rfc2863a.mib	ifTable ifXTable ifStackTable
	rfc2011a.mib	ipAddrTable ipNetToMediaTable
	rtmib.mib	ipForward (ipCidrRouteTable)
	rfc2665a.mib	dot3StatsTable dot3ControlTable dot3PauseTable
	rfc2495a.mib	dsx1ConfigTable dsx1CurrentTable dsx1IntervalTable dsx1TotalTable dsx1FarEndCurrentTable dsx1FarEndIntervalTable dsx1FarEndTotalTable dsx1FracTable ...

Table 52: Class 1 MIB Objects (Standard and Juniper MIBs) *(continued)*

Class	MIB	Objects
	rfc2496a.mib	dsx3 (dsx3ConfigTable)
	rfc2115a.mib	frDlcmiTable (and related MIB objects)
	rfc3592.mib	sonetMediumTable (and related MIB objects)
	rfc3020.mib	mfrMIB mfrBundleTable mfrMibBundleLinkObjects mfrBundleIfIndexMappingTable (and related MIB objects)
	ospf2mib.mib	All objects
	ospf2trap.mib	All objects
	bgpmib.mib	All objects
	rfc2819a.mib	Example: etherStatsTable

Table 52: Class 1 MIB Objects (Standard and Juniper MIBs) *(continued)*

Class	MIB	Objects
Class 1	rfc2863a.mib	Examples: ifXtable ifStackTable
	rfc2665a.mib	etherMIB
	rfc2515a.mib	atmMIB objects Examples: atmInterfaceConfTable atmVplTable atmVclTable
	rfc2465.mib	ip-v6mib Examples: ipv6IfTable ipv6AddrPrefixTable ipv6NetToMediaTable ipv6RouteTable
	rfc2787a.mib	vrrp mib
	rfc2932.mib	ipMRouteMIB ipMRouteStdMIB
	mroutemib.mib	ipMRoute1MIBObjects
	isismib.mib	isisMIB
	pimmib.mib	pimMIB
	msdpmib.mib	msdpmib
	jnx-if-extensions.mib	

Table 52: Class 1 MIB Objects (Standard and Juniper MIBs) *(continued)*

Class	MIB	Objects
		Examples: ifJnxTable ifChassisTable
	jnx-dcu.mib	jnxDCUs
	jnx-atm.mib	Examples: jnxAtmIfTable jnxAtmVCTable jnxAtmVpTable
	jnx-ipv4.mib	jnxipv4 Example: jnxIpv4AddrTable
	jnx-cos.mib	Examples: jnxCosIfqStatsTable jnxCosQstatTable
	jnx-scu.mib	Example: jnxScuStatsTable
	jnx-rpf.mib	Example: jnxRpfStatsTable
	jnx-pmon.mib	Example: jnxPMonFlowTable
	jnx-sonet.mib	Example: jnxSonetAlarmTable

Table 52: Class 1 MIB Objects (Standard and Juniper MIBs) *(continued)*

Class	MIB	Objects
Class 1	jnx-atm-cos.mib	Examples: jnxCosAtmVcTable jnxCosAtmVcScTable jnxCosAtmVcQstatsTable jnxCosAtmTrunkTable
	jnx-mac.mib	Example: jnxMacStatsTable
	jnx-services.mib	Example: jnxSvcFlowTableAggStatsTable
	jnx-coll.mib	jnxCollectorMIB Examples: jnxCollPicIfTable jnxCollFileEntry

Table 53 on page 722 shows Class 2 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 2 objects, all instances within a logical system are exposed. Data will not be segregated down to the routing instance level.

Table 53: Class 2 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 2	rfc3813.mib	mplsLsrStdMIB Examples: mplsInterfaceTable mplsInSegmentTable mplsOutSegmentTable mplsLabelStackTable mplsXCTable (and related MIB objects)
	igmpmib.mib	igmpStdMIB **NOTE:** The **igmpmib.mib** is the draft version of the IGMP Standard MIB in the experimental tree. Junos OS does not support the original IGMP Standard MIB.
	l3vpnmib.mib	mplsVpnmib
	jnx-mpls.mib	Example: mplsLspList
	jnx-ldp.mib	jnxLdp Example: jnxLdpStatsTable
	jnx-vpn.mib	jnxVpnMIB
	jnx-bgpmib2.mib	jnxBgpM2Experiment

Table 54 on page 723 shows Class 3 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 3, objects are exposed only for the default logical system.

Table 54: Class 3 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 3	rfc2819a.mib	rmonEvents alarmTable logTable eventTable agentxMIB
	rfc2925a.mib	pingmib
	rfc2925b.mib	tracerouteMIB
	jnxchassis.mib	jnxBoxAnatomy
	jnx-chassis-alarm.mib	jnxAlarms By default, SRX Series devices queries jnxAlarms mib only on the primary node of redundancy group 0 (RG0) and not on the secondary node.
	jnx-ping.mib	jnxPingMIB
	jnx-traceroute.mib	jnxTraceRouteMIB
	jnx-rmon.mib	jnxRmonAlarmTable
	jnx-cos.mib	Example: jnxCosFcTable
	jnx-cfgmgmt.mib	Example: jnxCfgMgmt
	jnx-sonetaps.mib	apsMIBObjects
	jnx-sp.mib	jnxSpMIB
	ggsn.mib	ejnmobileipABmib
	rfc1907.mib	snmpModules
	snmpModules	Examples: snmpMIB snmpFrameworkMIB

Table 55 on page 724 shows Class 4 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 4 objects, data is not segregated by routing instance. All instances are exposed.

Table 55: Class 4 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 4	system	Example: sysORTable
	rfc2011a.mib	ip (ipDefaultTTL, ipInReceives) icmp
	rfc2012a.mib	tcp tcpConnTable ipv6TcpConnTable
	rfc2013a.mib	udp udpTable ipv6UdpTable
	rfc2790a.mib	hrSystem
	rfc2287a.mib	sysApplOBJ
	jnx-firewall.mib	jnxFirewalls
	jnx-ipv6.mib	jnxIpv6

RELATED DOCUMENTATION

- Understanding SNMP Support for Routing Instances | 710
- Support Classes for MIB Objects | 725
- SNMP Traps Supported for Routing Instances | 726

Support Classes for MIB Objects

When a routing instance is specified, all routing-related MIB objects return data maintained by the routing instance in the request. For all other MIB objects, the data returned is segregated according to that routing instance. For example, only those interfaces assigned to that routing instance (for example, the logical interfaces [ifls] as well as their corresponding physical interfaces [ifds]) are exposed by the SNMP agent. Similarly, objects with an unambiguous attachment to an interface (for example, addresses) are segregated as well.

For those objects where the attachment is ambiguous (for example, objects in sysApplMIB), no segregation is done and all instances are visible in all cases.

Another category of objects is visible only when no logical system is specified (only within the default logical system) regardless of the routing instance within the default logical system. Objects in this category are Chassis MIB objects, objects in the SNMP group, RMON alarm, event and log groups, Ping MIB objects, configuration management objects, and V3 objects.

In summary, to support routing instances, MIB objects fall into one of the following categories:

- Class 1—Data is segregated according to the routing instance in the request. This is the most granular of the segregation classes.
- Class 2—Data is segregated according to the logical system specified in the request. The same data is returned for all routing instances that belong to a particular logical system. Typically, this applies to routing table objects where it is difficult to extract routing instance information or where routing instances do not apply.
- Class 3—Data is exposed only for the default logical system. The same set of data is returned for all routing instances that belong to the default logical system. If you specify another logical system (not the default), no data is returned. Typically this class applies to objects implemented in subagents that do not monitor logical system changes and register their objects using only the default context (for example, Chassis MIB objects).
- Class 4—Data is not segregated by routing instance. The same data is returned for all routing instances. Typically, this applies to objects implemented in subagents that monitor logical system changes and register or deregister all their objects for each logical system change. Objects whose values cannot be segregated by routing instance fall into this class.

See “SNMP MIBs Supported for Routing Instances” on page 713 for a list of the objects associated with each class.

RELATED DOCUMENTATION

Understanding SNMP Support for Routing Instances | 710

SNMP Traps Supported for Routing Instances | 726

SNMP Traps Supported for Routing Instances

You can restrict the trap receivers from receiving traps that are not related to the logical system networks to which they belong. To do this, include the **logical-system-trap-filter** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
logical-system-trap-filter;
```

If the **logical-system-trap-filter** statement is not included in the SNMP configuration, all traps are forwarded to the configured routing instance destinations. However, even when this statement is configured, the trap receiver associated with the default routing instance will receive all SNMP traps.

When configured under the trap-group object, all v1 and v2c traps that apply to routing instances (or interfaces belonging to a routing instance) have the routing instance name encoded in the community string. The encoding is identical to that used in request PDUs.

For traps configured under the v3 framework, the routing instance name is carried in the context field when the v3 message processing model has been configured. For other message processing models (v1 or v2c), the routing instance name is not carried in the trap message header (and not encoded in the community string).

RELATED DOCUMENTATION

- Understanding SNMP Support for Routing Instances | **710**
- Support Classes for MIB Objects | **725**
- SNMP MIBs Supported for Routing Instances | **713**

Identifying a Routing Instance

With this feature, routing instances are identified by either the context field in v3 requests or encoded in the community string in v1 or v2c requests.

When encoded in a community string, the routing instance name appears first and is separated from the actual community string by the @ character.

To avoid conflicts with valid community strings that contain the @ character, the community is parsed only if typical community string processing fails. For example, if a routing instance named **RI** is configured, an SNMP request with **RI@public** is processed within the context of the **RI** routing instance. Access control (views, source address restrictions, access privileges, and so on) is applied according to the actual community

string (the set of data after the @ character—in this case **public**). However, if the community string **RI@public** is configured, the protocol data unit (PDU) is processed according to that community and the embedded routing instance name is ignored.

Logical systems perform a subset of the actions of a physical router and have their own unique routing tables, interfaces, policies, and routing instances. When a routing instance is defined within a logical system, the logical system name must be encoded along with the routing instance using a slash (**/**) to separate the two. For example, if the routing instance **RI** is configured within the logical system **LS**, that routing instance must be encoded within a community string as **LS/RI@public**. When a routing instance is configured outside a logical system (within the default logical system), no logical system name (or **/** character) is needed.

Also, when a logical system is created, a default routing instance (named **default**) is always created within the logical system. This name should be used when querying data for that routing instance (for example, **LS/default@public**). For v3 requests, the name ***logical system/routing instance*** should be identified directly in the context field.

> **NOTE:** To identify a virtual LAN (VLAN) spanning-tree instance (VSTP on MX Series 5G Universal Routing Platforms), specify the routing instance name followed by a double colon (**::**) and the VLAN ID. For example, to identify VSTP instance for VLAN 10 in the global default routing instance, include **default::10@public** in the **context** (SNMPv3) or **community** (SNMPv1 or v2) string.

RELATED DOCUMENTATION

- Understanding SNMP Support for Routing Instances | **710**
- Enabling SNMP Access over Routing Instances | **727**
- Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | **728**

Enabling SNMP Access over Routing Instances

To enable SNMP managers in routing instances other than the default routing instance to access SNMP information, include the **routing-instance-access** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
routing-instance-access;
```

If this statement is not included in the SNMP configuration, SNMP managers from routing instances other than the default routing instance cannot access SNMP information. This setting applies to requests for any version of SNMP (SNMP v1, v2, or v3).

RELATED DOCUMENTATION

- Understanding SNMP Support for Routing Instances | 710
- Identifying a Routing Instance | 726
- Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728
- Configuring Access Lists for SNMP Access over Routing Instances | 731

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community

You can specify the routing instance along with the client information when you add a client to an SNMP community. To specify the routing instance to which a client belongs, include the **routing-instance** statement followed by the routing instance name and client information in the SNMP configuration.

The following example shows the configuration statement to add routing instance test-ri to SNMP community community1.

> **NOTE:** Routing instances specified at the **[edit snmp community *community-name*]** hierarchy level are added to the default logical system in the community.

```
[edit snmp]
community community1 {
    clients {
        10.209.152.33/32;
    }
    routing-instance test-ri {
        clients {
            10.19.19.1/32;
        }
    }
}
```

If the routing instance is defined within a logical system, include the **routing-instance** statement at the [**edit snmp community *community-name* logical-system *logical-system-name***] hierarchy level, as in the following example:

```
[edit snmp]
community community1 {
    clients {
        10.209.152.33/32;
    }
    logical-system test-LS {
        routing-instance test-ri {
            clients {
                10.19.19.1/32;
            }
        }
    }
}
```

RELATED DOCUMENTATION

- Understanding SNMP Support for Routing Instances | **710**
- Identifying a Routing Instance | **726**
- Enabling SNMP Access over Routing Instances | **727**
- Configuring Access Lists for SNMP Access over Routing Instances | **731**
- Example: Configuring Interface Settings for a Routing Instance | **729**

Example: Configuring Interface Settings for a Routing Instance

This example shows an 802.3ad ae0 interface configuration allocated to a routing instance named INFrtd:

```
[edit chassis]
aggregated-devices {
    ethernet {
        device-count 5;
    }
}
[edit interfaces ae0]
vlan-tagging;
```

```
aggregated-ether-options {
    minimum-links 2;
    link-speed 100m;
}
unit 0 {
    vlan-id 100;
    family inet {
        address 10.1.0.1/24;
    }
}
[edit interfaces fe-1/1/0]
fastether-options {
    802.3ad ae0;
}
[edit interfaces fe-1/1/1]
fastether-options {
    802.3ad ae0;
}
[edit routing-instances]
INFrtd {
    instance-type virtual-router;
    interface fe-1/1/0.0;
    interface fe-1/1/1.0;
    interface fe-1/1/5.0;
    interface ae0.0;
    protocols {
        ospf {
            area 0.0.0.0 {
                interface all;
            }
        }
    }
}
```

The following **snmpwalk** command shows how to retrieve SNMP-related information from router1 and the 802.3ae bundle interface belonging to routing instance INFrtd with the SNMP community **public**:

```
router# snmpwalk -Os router1 INFrtd@public dot3adAggTable
dot3adAggMACAddress.59 = 0:90:69:92:93:f0
dot3adAggMACAddress.65 = 0:90:69:92:93:f0
dot3adAggActorSystemPriority.59 = 0
dot3adAggActorSystemPriority.65 = 0
dot3adAggActorSystemID.59 = 0:0:0:0:0:0
dot3adAggActorSystemID.65 = 0:0:0:0:0:0
```

```
dot3adAggAggregateOrIndividual.59 = true(1)
dot3adAggAggregateOrIndividual.65 = true(1)
dot3adAggActorAdminKey.59 = 0
dot3adAggActorAdminKey.65 = 0
dot3adAggActorOperKey.59 = 0
dot3adAggActorOperKey.65 = 0
dot3adAggPartnerSystemID.59 = 0:0:0:0:0:0
dot3adAggPartnerSystemID.65 = 0:0:0:0:0:0
dot3adAggPartnerSystemPriority.59 = 0
dot3adAggPartnerSystemPriority.65 = 0
dot3adAggPartnerOperKey.59 = 0
dot3adAggPartnerOperKey.65 = 0
dot3adAggCollectorMaxDelay.59 = 0
dot3adAggCollectorMaxDelay.65 = 0
```

RELATED DOCUMENTATION

Understanding SNMP Support for Routing Instances | 710

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728

Configuring Access Lists for SNMP Access over Routing Instances

You can create and maintain access lists to manage access to SNMP information. Access list configuration enables you to allow or deny SNMP access to clients of a specific routing instance, and applies to requests for any version of SNMP.

The following example shows how to create an access list:

```
[edit snmp]
routing-instance-access {
    access-list {
        ri1 restrict;
        ls1/default;
        ls1/ri2;
        ls1*;
    }
}
```

The configuration given in the example:

- Restricts clients in **ri1** from accessing SNMP information.
- Allows clients in **ls1/default**, **ls1/ri2**, and all other routing instances with names starting with **ls1** to access SNMP information.

You can use the wildcard character (*) to represent a string in the routing instance name.

> **NOTE:** You cannot restrict the SNMP manager of the default routing instance from accessing SNMP information.

RELATED DOCUMENTATION

Understanding SNMP Support for Routing Instances | **710**

Enabling SNMP Access over Routing Instances | **727**

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | **728**

SNMPv3 Management Routing Instance

Starting in Junos OS 19.4R1, you can access information related to all routing instances and logical system networks and not specific to ingress routing instance by configuring the SNMPv3 management interface in a required management instance. You can configure the management instance configuration statement at the **[edit SNMP v3]** hierarchy level.

Benefits

SNMPv3 management routing instance enables all the SNMPv3 requests from non-default routing instance as if the requests are from default routing instance. Using SNMPv3 management routing instance, you access the information related to all routing instances and logical system networks.

Enabling the Management Routing Instance

To enable the SNMPv3 management routing instance:

1. Configure the management-instance statement.

   [edit]

```
user@host# set SNMP v3 management-routing-instance <routing-instance>
```

2. Commit the configuration.

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

Removing the Management Routing Instance

To remove the SNMPv3 management routing instance:

1. Delete or deactivate the SNMPv3 management routing instance statement.

```
[edit]
user@host# delete SNMP v3 management-routing-instance <routing-instance>
```

RELATED DOCUMENTATION

Understanding SNMP Support for Routing Instances | 710

CHAPTER 17

Configuring SNMP Remote Operations

IN THIS CHAPTER

- SNMP Remote Operations Overview | 734
- Using the Ping MIB for Remote Monitoring Devices Running Junos OS | 738
- Starting a Ping Test | 739
- Monitoring a Running Ping Test | 741
- Gathering Ping Test Results | 744
- Stopping a Ping Test | 746
- Interpreting Ping Variables | 746
- Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747
- Starting a Traceroute Test | 747
- Monitoring a Running Traceroute Test | 749
- Monitoring Traceroute Test Completion | 753
- Gathering Traceroute Test Results | 754
- Stopping a Traceroute Test | 756
- Interpreting Traceroute Variables | 756

SNMP Remote Operations Overview

IN THIS SECTION

- SNMP Remote Operation Requirements | 735
- Setting SNMP Views | 735
- Setting Trap Notification for Remote Operations | 736
- Using Variable-Length String Indexes | 737
- Enabling Logging | 737

A SNMP remote operation is any process on the router that can be controlled remotely using SNMP. Junos OS currently provides support for two SNMP remote operations: the Ping MIB and Traceroute MIB, defined in RFC 2925. Using these MIBs, an SNMP client in the network management system (NMS) can:

- Start a series of operations on a router
- Receive notification when the operations are complete
- Gather the results of each operation

Junos OS also provides extended functionality to these MIBs in the Juniper Networks enterprise-specific extensions **jnxPingMIB** and **jnxTraceRouteMIB**. For more information about **jnxPingMIB** and **jnxTraceRouteMIB**, see PING MIB and Traceroute MIB.

This topic covers the following sections:

SNMP Remote Operation Requirements

To use SNMP remote operations, you should be experienced with SNMP conventions. You must also configure Junos OS to allow the use of the remote operation MIBs.

Before starting the Ping MIB, see "Starting a Ping Test" on page 739.

Before starting the Traceroute MIB, see "Starting a Traceroute Test" on page 747.

Setting SNMP Views

All remote operation MIBs supported by Junos OS require that the SNMP clients have read-write privileges. The default SNMP configuration of Junos OS does not provide clients with a community string with such privileges.

To set read-write privileges for an SNMP community string, include the following statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
community community-name {
    authorization authorization;
    view view-name;
}
view view-name {
    oid object-identifier (include | exclude);
}
```

Example: Setting SNMP Views

To create a community named **remote-community** that grants SNMP clients read-write access to the Ping MIB, **jnxPing** MIB, Traceroute MIB, and **jnxTraceRoute** MIB, include the following statements at the **[edit snmp]** hierarchy level:

```
snmp {
    view remote-view {
        oid 1.3.6.1.2.1.80 include; # pingMIB
        oid 1.3.6.1.4.1.2636.3.7 include; # jnxPingMIB
        oid 1.3.6.1.2.1.81 include; # traceRouteMIB
        oid 1.3.6.1.4.1.2636.3.8 include; # jnxTraceRouteMIB
    }
    community remote-community {
        view remote-view;
        authorization read-write;
    }
}
```

For more information about the **community** statement, see "Configuring SNMP Communities" on page 573 and **community (SNMP)**.

For more information about the **view** statement, see "Configuring MIB Views" on page 612, **view (SNMP Community)**, and **view (Configuring a MIB View)**.

Setting Trap Notification for Remote Operations

In addition to configuring the remote operations MIB for trap notification, you must also configure Junos OS. You must specify a target host for remote operations traps.

To configure trap notification for SNMP remote operations, include the **categories** and **targets** statements at the **[edit snmp trap-group *group-name*]** hierarchy level:

```
[edit snmp trap-group group-name]
    categories {
        category;
    }
    targets {
        address;
    }
}
```

Example: Setting Trap Notification for Remote Operations

Specify **172.17.12.213** as a target host for all remote operation traps:

```
snmp {
    trap-group remote-traps {
        categories remote-operations;
        targets {
            172.17.12.213;
        }
    }
}
```

For more information about trap groups, see "Configuring SNMP Trap Groups" on page 591.

Using Variable-Length String Indexes

All tabular objects in the remote operations MIBs supported by Junos OS are indexed by two variables of type **SnmpAdminString**. For more information about **SnmpAdminString**, see RFC 2571.

Junos OS does not handle **SnmpAdminString** any differently from the octet string variable type. However, the indexes are defined as variable length. When a variable length string is used as an index, the length of the string must be included as part of the object identifier (OID).

Example: Set Variable-Length String Indexes

To reference the **pingCtlTargetAddress** variable of a row in **pingCtlTable** where **pingCtlOwnerIndex** is **bob** and **pingCtlTestName** is **test**, use the following object identifier (OID):

```
pingMIB.pingObjects.pingCtlTable.pingCtlEntry.pingCtlTargetAddress."bob"."test"
1.3.6.1.2.1.80.1.2.1.4.3.98.111.98.4.116.101.115.116
```

For more information about the definition of the Ping MIB, see RFC 2925.

Enabling Logging

The SNMP error code returned in response to SNMP requests can only provide a generic description of the problem. The error descriptions logged by the remote operations process can often provide more detailed information about the problem and help you to solve the problem faster. This logging is not enabled by default. To enable logging, include the **flag general** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit]
```

```
snmp {
    traceoptions {
        flag general;
    }
}
```

For more information about traceoptions, see "Tracing SNMP Activity on a Device Running Junos OS" on page 766.

If the remote operations process receives an SNMP request that it cannot accommodate, the error is logged in the **/var/log/rmopd** file. To monitor this log file, issue the **monitor start rmopd** command in operational mode of the command-line interface (CLI).

RELATED DOCUMENTATION

- Using the Ping MIB for Remote Monitoring Devices Running Junos OS | **738**
- Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | **747**

Using the Ping MIB for Remote Monitoring Devices Running Junos OS

A ping test is used to determine whether packets sent from the local host reach the designated host and are returned. If the designated host can be reached, the ping test provides the approximate round-trip time for the packets. Ping test results are stored in **pingResultsTable** and **pingProbeHistoryTable**.

RFC 2925 is the authoritative description of the Ping MIB in detail and provides the ASN.1 MIB definition of the Ping MIB.

RELATED DOCUMENTATION

- SNMP Remote Operations Overview | **734**
- Starting a Ping Test | **739**
- Monitoring a Running Ping Test | **741**
- Gathering Ping Test Results | **744**
- Stopping a Ping Test | **746**
- Interpreting Ping Variables | **746**

Starting a Ping Test

IN THIS SECTION

- Before You Begin | 739
- Starting a Ping Test | 739
- Using Multiple Set PDUs | 740
- Using a Single Set PDU | 740

Use this topic to launch an ICMP ping test. There are two ways to start a ping test: using multiple Set protocol data units (PDUs) or using a single Set PDU.

Before You Begin

Before you start a ping test, configure a Ping MIB view. This allows SNMP **Set** requests on **pingMIB**. For more information, see "Configuring MIB Views" on page 612.

Starting in Junos OS Release 17.2X75-D100, you must configure RPM before starting an ICMP ping. Configure RPM using the **edit services rpm** command.

Starting a Ping Test

To start a ping test, create a row in **pingCtlTable** and set **pingCtlAdminStatus** to **enabled**. The minimum information that must be specified before setting **pingCtlAdminStatus** to **enabled** is:

- **pingCtlOwnerIndexSnmpAdminString**
- **pingCtlTestNameSnmpAdminString**
- **pingCtlTargetAddressInetAddress**
- **pingCtlTargetAddressTypeInetAddressType**
- **pingCtlRowStatusRowStatus**

For all other values, defaults are chosen unless otherwise specified. **pingCtlOwnerIndex** and **pingCtlTestName** are used as the index, so their values are specified as part of the object identifier (OID). To create a row, set **pingCtlRowStatus** to **createAndWait** or **createAndGo** on a row that does not already exist. A value of **active** for **pingCtlRowStatus** indicates that all necessary information has been supplied and the test can begin; **pingCtlAdminStatus** can be set to **enabled**. An SNMP **Set** request that sets **pingCtlRowStatus** to **active** will fail if the necessary information in the row is not specified or is inconsistent.

For information about how to configure a view, see “Setting SNMP Views” on page 735.

Read the following sections for how to order the variables.

Using Multiple Set PDUs

You can use multiple **Set** request PDUs (multiple PDUs, with one or more varbinds each) and set the following variables in this order to start the test:

- **pingCtlRowStatus** to **createAndWait**
- All appropriate test variables
- **pingCtlRowStatus** to **active**

  Junos OS now verifies that all necessary information to run a test has been specified.
- **pingCtlAdminStatus** to **enabled**

Using a Single Set PDU

You can use a single **Set** request PDU (one PDU, with multiple varbinds) to set the following variables to start the test:

- **pingCtlRowStatus** to **createAndGo**
- All appropriate test variables
- **pingCtlAdminStatus** to **enabled**

Release History Table

Release	Description
17.2X75-D100	Starting in Junos OS Release 17.2X75-D100, you must configure RPM before starting an ICMP ping.

RELATED DOCUMENTATION

Setting SNMP Views | 735

Monitoring a Running Ping Test

IN THIS SECTION

- pingResultsTable | 741
- pingProbeHistoryTable | 743
- Generating Traps | 743

When **pingCtlAdminStatus** is successfully set to **enabled**, the following is done before the acknowledgment of the SNMP **Set** request is sent back to the client:

- **pingResultsEntry** is created if it does not already exist.
- **pingResultsOperStatus** transitions to **enabled**.

For more information, see the following sections:

pingResultsTable

While the test is running, **pingResultsEntry** keeps track of the status of the test. The value of **pingResultsOperStatus** is **enabled** while the test is running and **disabled** when it has stopped.

The value of **pingCtlAdminStatus** remains **enabled** until you set it to **disabled**. Thus, to get the status of the test, you must examine **pingResultsOperStatus**.

The **pingCtlFrequency** variable can be used to schedule many tests for one **pingCtlEntry**. After a test ends normally (you did not stop the test) and the **pingCtlFrequency** number of seconds has elapsed, the test is started again just as if you had set **pingCtlAdminStatus** to **enabled**. If you intervene at any time between repeated tests (you set **pingCtlAdminStatus** to **disabled** or **pingCtlRowStatus** to **notInService**), the repeat feature is disabled until another test is started and ends normally. A value of 0 for **pingCtlFrequency** indicates this repeat feature is not active.

pingResultsIpTgtAddr and **pingResultsIpTgtAddrType** are set to the value of the resolved destination address when the value of **pingCtlTargetAddressType** is **dns**. When a test starts successfully and **pingResultsOperStatus** transitions to **enabled**:

- **pingResultsIpTgtAddr** is set to **null-string**.
- **pingResultsIpTgtAddrType** is set to **unknown**.

pingResultsIpTgtAddr and **pingResultsIpTgtAddrType** are not set until **pingCtlTargetAddress** can be resolved to a numeric address. To retrieve these values, poll **pingResultsIpTgtAddrType** for any value other than **unknown** after successfully setting **pingCtlAdminStatus** to **enabled**.

At the start of a test, **pingResultsSentProbes** is initialized to 1 and the first probe is sent. **pingResultsSentProbes** increases by 1 each time a probe is sent.

As the test runs, every **pingCtlTimeOut** seconds, the following occur:

- **pingProbeHistoryStatus** for the corresponding **pingProbeHistoryEntry** in **pingProbeHistoryTable** is set to **requestTimedOut**.
- A **pingProbeFailed** trap is generated, if necessary.
- An attempt is made to send the next probe.

> **NOTE:** No more than one outstanding probe exists for each test.

For every probe, you can receive one of the following results:

- The target host acknowledges the probe with a response.
- The probe times out; there is no response from the target host acknowledging the probe.
- The probe could not be sent.

Each probe result is recorded in **pingProbeHistoryTable**. For more information about **pingProbeHistoryTable**, see "pingProbeHistoryTable" on page 743.

When a response is received from the target host acknowledging the current probe:

- **pingResultsProbeResponses** increases by 1.
- The following variables are updated:
  - **pingResultsMinRtt**—Minimum round-trip time
  - **pingResultsMaxRtt**—Maximum round-trip time
  - **pingResultsAverageRtt**—Average round-trip time
  - **pingResultsRttSumOfSquares**—Sum of squares of round-trip times
  - **pingResultsLastGoodProbe**—Timestamp of the last response

> **NOTE:** Only probes that result in a response from the target host contribute to the calculation of the round-trip time (RTT) variables.

When a response to the last probe is received or the last probe has timed out, the test is complete.

pingProbeHistoryTable

An entry in **pingProbeHistoryTable** (**pingProbeHistoryEntry**) represents a probe result and is indexed by three variables:

- The first two variables, **pingCtlOwnerIndex** and **pingCtlTestName**, are the same ones used for **pingCtlTable**, which identifies the test.
- The third variable, **pingProbeHistoryIndex**, is a counter to uniquely identify each probe result.

The maximum number of **pingProbeHistoryTable** entries created for a given test is limited by **pingCtlMaxRows**. If **pingCtlMaxRows** is set to 0, no **pingProbeHistoryTable** entries are created for that test.

Each time a probe result is determined, a **pingProbeHistoryEntry** is created and added to **pingProbeHistoryTable**. **pingProbeHistoryIndex** of the new **pingProbeHistoryEntry** is 1 greater than the last **pingProbeHistoryEntry** added to **pingProbeHistoryTable** for that test. **pingProbeHistoryIndex** is set to 1 if this is the first entry in the table. The same test can be run multiple times, so this index keeps growing.

If **pingProbeHistoryIndex** of the last **pingProbeHistoryEntry** added is 0xFFFFFFFF, the next **pingProbeHistoryEntry** added has **pingProbeHistoryIndex** set to 1.

The following are recorded for each probe result:

- **pingProbeHistoryResponse**—Time to live (TTL)
- **pingProbeHistoryStatus**—What happened and why
- **pingProbeHistoryLastRC**—Return code (RC) value of ICMP packet
- **pingProbeHistoryTime**—Timestamp when probe result was determined

When a probe cannot be sent, **pingProbeHistoryResponse** is set to 0. When a probe times out, **pingProbeHistoryResponse** is set to the difference between the time when the probe was discovered to be timed out and the time when the probe was sent.

Generating Traps

For any trap to be generated, the appropriate bit of **pingCtlTrapGeneration** must be set. You must also configure a trap group to receive remote operations. A trap is generated under the following conditions:

- A **pingProbeFailed** trap is generated every time **pingCtlTrapProbeFailureFilter** number of consecutive probes fail during the test.
- A **pingTestFailed** trap is generated when the test completes and at least **pingCtlTrapTestFailureFilter** number of probes fail.

- A **pingTestCompleted** trap is generated when the test completes and fewer than **pingCtlTrapTestFailureFilter** probes fail.

> **NOTE:** A probe is considered a failure when **pingProbeHistoryStatus** of the probe result is anything besides **responseReceived**.

For information about how to configure a trap group to receive remote operations, see "Configuring SNMP Trap Groups" on page 591 and "Example: Setting Trap Notification for Remote Operations" on page 737.

Gathering Ping Test Results

You can either poll **pingResultsOperStatus** to find out when the test is complete or request that a trap be sent when the test is complete. For more information about **pingResultsOperStatus**, see "pingResultsTable" on page 741. For more information about Ping MIB traps, see "Generating Traps" on page 743.

The statistics calculated and then stored in **pingResultsTable** include:

- **pingResultsMinRtt**—Minimum round-trip time
- **pingResultsMaxRtt**—Maximum round-trip time
- **pingResultsAverageRtt**—Average round-trip time
- **pingResultsProbeResponses**—Number of responses received
- **pingResultsSentProbes**—Number of attempts to send probes
- **pingResultsRttSumOfSquares**—Sum of squares of round-trip times
- **pingResultsLastGoodProbe**—Timestamp of the last response

You can also consult **pingProbeHistoryTable** for more detailed information about each probe. The index used for **pingProbeHistoryTable** starts at 1, goes to 0xFFFFFFFF, and wraps to 1 again.

For example, if **pingCtlProbeCount** is 15 and **pingCtlMaxRows** is 5, then upon completion of the first run of this test, **pingProbeHistoryTable** contains probes like those in Table 56 on page 744.

Table 56: Results in pingProbeHistoryTable: After the First Ping Test

pingProbeHistoryIndex	Probe Result
11	Result of 11th probe from run 1
12	Result of 12th probe from run 1

Table 56: Results in pingProbeHistoryTable: After the First Ping Test *(continued)*

pingProbeHistoryIndex	Probe Result
13	Result of 13th probe from run 1
14	Result of 14th probe from run 1
15	Result of 15th probe from run 1

Upon completion of the first probe of the second run of this test, **pingProbeHistoryTable** will contain probes like those in Table 57 on page 745.

Table 57: Results in pingProbeHistoryTable: After the First Probe of the Second Test

pingProbeHistoryIndex	Probe Result
12	Result of 12th probe from run 1
13	Result of 13th probe from run 1
14	Result of 14th probe from run 1
15	Result of 15th probe from run 1
16	Result of 1st probe from run 2

Upon completion of the second run of this test, **pingProbeHistoryTable** will contain probes like those in Table 58 on page 745.

Table 58: Results in pingProbeHistoryTable: After the Second Ping Test

pingProbeHistoryIndex	Probe Result
26	Result of 11th probe from run 2
27	Result of 12th probe from run 2
28	Result of 13th probe from run 2
29	Result of 14th probe from run 2
30	Result of 15th probe from run 2

History entries can be deleted from the MIB in two ways:

- More history entries for a given test are added and the number of history entries exceeds **pingCtlMaxRows**. The oldest history entries are deleted to make room for the new ones.
- You delete the entire test by setting **pingCtlRowStatus** to **destroy**.

Stopping a Ping Test

To stop an active test, set **pingCtlAdminStatus** to **disabled**. To stop the test and remove its **pingCtlEntry**, **pingResultsEntry**, and any **pingHistoryEntry** objects from the MIB, set **pingCtlRowStatus** to **destroy**.

Interpreting Ping Variables

This section clarifies the ranges for the following variables that are not explicitly specified in the Ping MIB:

- **pingCtlDataSize**—The value of this variable represents the total size of the payload (in bytes) of an outgoing probe packet. This payload includes the timestamp (8 bytes) that is used to time the probe. This is consistent with the definition of **pingCtlDataSize** (maximum value of 65,507) and the standard ping application.

  If the value of **pingCtlDataSize** is between 0 and 8 inclusive, it is ignored and the payload is 8 bytes (the timestamp). The Ping MIB assumes all probes are timed, so the payload must always include the timestamp.

  For example, if you wish to add an additional 4 bytes of payload to the packet, you must set **pingCtlDataSize** to 12.
- **pingCtlDataFill**—The first 8 bytes of the data segment of the packet is for the timestamp. After that, the **pingCtlDataFill** pattern is used in repetition. The default pattern (when **pingCtlDataFill** is not specified) is (00, 01, 02, 03 ... FF, 00, 01, 02, 03 ... FF, ...).
- **pingCtlMaxRows**—The maximum value is 255.
- **pingMaxConcurrentRequests**—The maximum value is 500.
- **pingCtlTrapProbeFailureFilter** and **pingCtlTrapTestFailureFilter**—A value of 0 for **pingCtlTrapProbeFailureFilter** or **pingCtlTrapTestFailureFilter** is not well defined by the Ping MIB. If **pingCtlTrapProbeFailureFilter** is 0, **pingProbeFailed** traps will not be generated for the test under any circumstances. If **pingCtlTrapTestFailureFilter** is 0, **pingTestFailed** traps will not be generated for the test under any circumstances.

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS

A traceroute test approximates the path packets take from the local host to the remote host.

RFC 2925 is the authoritative description of the Traceroute MIB in detail and provides the ASN.1 MIB definition of the Traceroute MIB.

RELATED DOCUMENTATION

- SNMP Remote Operations Overview | 734
- Starting a Traceroute Test | 747
- Monitoring a Running Traceroute Test | 749
- Monitoring Traceroute Test Completion | 753
- Gathering Traceroute Test Results | 754
- Stopping a Traceroute Test | 756
- Interpreting Traceroute Variables | 756

Starting a Traceroute Test

IN THIS SECTION

- Using Multiple Set PDUs | 748
- Using a Single Set PDU | 748

Before you start a traceroute test, configure a Traceroute MIB view. This allows SNMP **Set** requests on **tracerouteMIB**. To start a test, create a row in **traceRouteCtlTable** and set **traceRouteCtlAdminStatus** to **enabled**. You must specify at least the following before setting **traceRouteCtlAdminStatus** to **enabled**:

- **traceRouteCtlOwnerIndexSnmpAdminString**
- **traceRouteCtlTestNameSnmpAdminString**
- **traceRouteCtlTargetAddressInetAddress**
- **traceRouteCtlRowStatusRowStatus**

For all other values, defaults are chosen unless otherwise specified. **traceRouteCtlOwnerIndex** and **traceRouteCtlTestName** are used as the index, so their values are specified as part of the OID. To create a row, set **traceRouteCtlRowStatus** to **createAndWait** or **createAndGo** on a row that does not already exist. A value of **active** for **traceRouteCtlRowStatus** indicates that all necessary information has been specified and the test can begin; **traceRouteCtlAdminStatus** can be set to **enabled**. An SNMP **Set** request that sets **traceRouteCtlRowStatus** to **active** will fail if the necessary information in the row is not specified or is inconsistent. For information about how to configure a view, see "Setting SNMP Views" on page 735.

There are two ways to start a traceroute test:

Using Multiple Set PDUs

You can use multiple **Set** request PDUs (multiple PDUs, with one or more varbinds each) and set the following variables in this order to start the test:

- **traceRouteCtlRowStatus** to createAndWait
- All appropriate test variables
- **traceRouteCtlRowStatus** to **active**

  The Junos OS now verifies that all necessary information to run a test has been specified.
- **traceRouteCtlAdminStatus** to **enabled**

Using a Single Set PDU

You can use a single **Set** request PDU (one PDU, with multiple varbinds) to set the following variables to start the test:

- **traceRouteCtlRowStatus** to **createAndGo**
- All appropriate test variables
- **traceRouteCtlAdminStatus** to enabled

RELATED DOCUMENTATION

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747

Monitoring a Running Traceroute Test | 749

SNMP Remote Operations Overview | 734

Monitoring Traceroute Test Completion | 753

Gathering Traceroute Test Results | 754

Stopping a Traceroute Test | 756

Interpreting Traceroute Variables | 756

Monitoring a Running Traceroute Test

IN THIS SECTION

- traceRouteResultsTable | 749
- traceRouteProbeResultsTable | 750
- traceRouteHopsTable | 751
- Generating Traps | 752

When traceRouteCtlAdminStatus is successfully set to enabled, the following is done before the acknowledgment of the SNMP Set request is sent back to the client:

- traceRouteResultsEntry is created if it does not already exist.
- traceRouteResultsOperStatus transitions to enabled.

For more information, see the following sections:

traceRouteResultsTable

While the test is running, this traceRouteResultsTable keeps track of the status of the test. The value of traceRouteResultsOperStatus is enabled while the test is running and disabled when it has stopped.

The value of traceRouteCtlAdminStatus remains enabled until you set it to disabled. Thus, to get the status of the test, you must examine traceRouteResultsOperStatus.

The traceRouteCtlFrequency variable can be used to schedule many tests for one traceRouteCtlEntry. After a test ends normally (you did not stop the test) and traceRouteCtlFrequency number of seconds has elapsed, the test is started again just as if you had set traceRouteCtlAdminStatus to enabled. If you intervene at any time between repeated tests (you set traceRouteCtlAdminStatus to disabled or traceRouteCtlRowStatus to notInService), the repeat feature is disabled until another test is started and ends normally. A value of 0 for traceRouteCtlFrequency indicates this repeat feature is not active.

traceRouteResultsIpTgtAddr and traceRouteResultsIpTgtAddrType are set to the value of the resolved destination address when the value of traceRouteCtlTargetAddressType is dns. When a test starts successfully and traceRouteResultsOperStatus transitions to enabled:

- traceRouteResultsIpTgtAddr is set to null-string.

- traceRouteResultsIpTgtAddrType is set to unknown.

traceRouteResultsIpTgtAddr and traceRouteResultsIpTgtAddrType are not set until traceRouteCtlTargetAddress can be resolved to a numeric address. To retrieve these values, poll traceRouteResultsIpTgtAddrType for any value other than unknown after successfully setting traceRouteCtlAdminStatus to enabled.

At the start of a test, traceRouteResultsCurHopCount is initialized to traceRouteCtlInitialTtl, and traceRouteResultsCurProbeCount is initialized to 1. Each time a probe result is determined, traceRouteResultsCurProbeCount increases by 1. While the test is running, the value of traceRouteResultsCurProbeCount reflects the current outstanding probe for which results have not yet been determined.

The traceRouteCtlProbesPerHop number of probes is sent for each time-to-live (TTL) value. When the result of the last probe for the current hop is determined, provided that the current hop is not the destination hop, traceRouteResultsCurHopCount increases by 1, and traceRouteResultsCurProbeCount resets to 1.

At the start of a test, if this is the first time this test has been run for this traceRouteCtlEntry, traceRouteResultsTestAttempts and traceRouteResultsTestSuccesses are initialized to 0.

At the end of each test execution, traceRouteResultsOperStatus transitions to disabled, and traceRouteResultsTestAttempts increases by 1. If the test was successful in determining the full path to the target, traceRouteResultsTestSuccesses increases by 1, and traceRouteResultsLastGoodPath is set to the current time.

traceRouteProbeResultsTable

Each entry in traceRouteProbeHistoryTable is indexed by five variables:

- The first two variables, traceRouteCtlOwnerIndex and traceRouteCtlTestName, are the same ones used for traceRouteCtlTable and to identify the test.
- The third variable, traceRouteProbeHistoryIndex, is a counter, starting from 1 and wrapping at FFFFFFFF. The maximum number of entries is limited by traceRouteCtlMaxRows.
- The fourth variable, traceRouteProbeHistoryHopIndex, indicates which hop this probe is for (the actual time-to-live or TTL value). Thus, the first traceRouteCtlProbesPerHop number of entries created when a test starts have a value of traceRouteCtlInitialTtl for traceRouteProbeHistoryHopIndex.
- The fifth variable, traceRouteProbeHistoryProbeIndex, is the probe for the current hop. It ranges from 1 to traceRouteCtlProbesPerHop.

While a test is running, as soon as a probe result is determined, the next probe is sent. A maximum of traceRouteCtlTimeOut seconds elapses before a probe is marked with status requestTimedOut and the next probe is sent. There is never more than one outstanding probe per traceroute test. Any probe result coming back after a probe times out is ignored.

Each probe can:

- Result in a response from a host acknowledging the probe
- Time out with no response from a host acknowledging the probe
- Fail to be sent

Each probe status is recorded in traceRouteProbeHistoryTable with traceRouteProbeHistoryStatus set accordingly.

Probes that result in a response from a host record the following data:

- traceRouteProbeHistoryResponse—Round-trip time (RTT)
- traceRouteProbeHistoryHAddrType—The type of HAddr (next argument)
- traceRouteProbeHistoryHAddr—The address of the hop

All probes, regardless of whether a response for the probe is received, have the following recorded:

- traceRouteProbeHistoryStatus—What happened and why
- traceRouteProbeHistoryLastRC—Return code (RC) value of the ICMP packet
- traceRouteProbeHistoryTime—Timestamp when the probe result was determined

When a probe cannot be sent, traceRouteProbeHistoryResponse is set to 0. When a probe times out, traceRouteProbeHistoryResponse is set to the difference between the time when the probe was discovered to be timed out and the time when the probe was sent.

traceRouteHopsTable

Entries in traceRouteHopsTable are indexed by three variables:

- The first two, traceRouteCtlOwnerIndex and traceRouteCtlTestName, are the same ones used for traceRouteCtlTable and identify the test.
- The third variable, traceRouteHopsHopIndex, indicates the current hop, which starts at 1 (not traceRouteCtlInitialTtl).

When a test starts, all entries in traceRouteHopsTable with the given traceRouteCtlOwnerIndex and traceRouteCtlTestName are deleted. Entries in this table are only created if traceRouteCtlCreateHopsEntries is set to true.

A new traceRouteHopsEntry is created each time the first probe result for a given TTL is determined. The new entry is created whether or not the first probe reaches a host. The value of traceRouteHopsHopIndex is increased by 1 for this new entry.

> **NOTE:** Any traceRouteHopsEntry can lack a value for traceRouteHopsIpTgtAddress if there are no responses to the probes with the given TTL.

Each time a probe reaches a host, the IP address of that host is available in the probe result. If the value of traceRouteHopsIpTgtAddress of the current traceRouteHopsEntry is not set, then the value of traceRouteHopsIpTgtAddress is set to this IP address. If the value of traceRouteHopsIpTgtAddress of the current traceRouteHopsEntry is the same as the IP address, then the value does not change. If the value of traceRouteHopsIpTgtAddress of the current traceRouteHopsEntry is different from this IP address, indicating a path change, a new traceRouteHopsEntry is created with:

- traceRouteHopsHopIndex variable increased by 1
- traceRouteHopsIpTgtAddress set to the IP address

> **NOTE:** A new entry for a test is added to traceRouteHopsTable each time a new TTL value is used or the path changes. Thus, the number of entries for a test may exceed the number of different TTL values used.

When a probe result is determined, the value traceRouteHopsSentProbes of the current traceRouteHopsEntry increases by 1. When a probe result is determined, and the probe reaches a host:

- The value traceRouteHopsProbeResponses of the current traceRouteHopsEntry is increased by 1.
- The following variables are updated:
  - traceRouteResultsMinRtt—Minimum round-trip time
  - traceRouteResultsMaxRtt—Maximum round-trip time
  - traceRouteResultsAverageRtt—Average round-trip time
  - traceRouteResultsRttSumOfSquares—Sum of squares of round-trip times
  - traceRouteResultsLastGoodProbe—Timestamp of the last response

> **NOTE:** Only probes that reach a host affect the round-trip time values.

Generating Traps

For any trap to be generated, the appropriate bit of traceRouteCtlTrapGeneration must be set. You must also configure a trap group to receive remote operations. Traps are generated under the following conditions:

- traceRouteHopsIpTgtAddress of the current probe is different from the last probe with the same TTL value (traceRoutePathChange).
- A path to the target could not be determined (traceRouteTestFailed).

A path to the target was determined (traceRouteTestCompleted).

For information about how to configure a trap group to receive remote operations, see "Configuring SNMP Trap Groups" on page 591 and "Example: Setting Trap Notification for Remote Operations" on page 737.

SEE ALSO

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747

SNMP Remote Operations Overview | 734

Starting a Traceroute Test | 747

Monitoring Traceroute Test Completion | 753

Gathering Traceroute Test Results | 754

Stopping a Traceroute Test | 756

Interpreting Traceroute Variables | 756

Monitoring Traceroute Test Completion

When a test is complete, **traceRouteResultsOperStatus** transitions from **enabled** to **disabled**. This transition occurs in the following situations:

- The test ends successfully. A probe result indicates that the destination has been reached. In this case, the current hop is the last hop. The rest of the probes for this hop are sent. When the last probe result for the current hop is determined, the test ends.
- **traceRouteCtlMaxTtl** threshold is exceeded. The destination is never reached. The test ends after the number of probes with TTL value equal to **traceRouteCtlMaxttl** have been sent.
- **traceRouteCtlMaxFailures** threshold is exceeded. The number of consecutive probes that end with status **requestTimedOut** exceeds **traceRouteCtlMaxFailures**.
- You end the test. You set **traceRouteCtlAdminStatus** to **disabled** or delete the row by setting **traceRouteCtlRowStatus** to **destroy**.
- You misconfigured the traceroute test. A value or variable you specified in **traceRouteCtlTable** is incorrect and will not allow a single probe to be sent. Because of the nature of the data, this error could not be determined until the test was started; that is, until after **traceRouteResultsOperStatus** transitioned to **enabled**. When this occurs, one entry is added to **traceRouteProbeHistoryTable** with **traceRouteProbeHistoryStatus** set to the appropriate error code.

If **traceRouteCtlTrapGeneration** is set properly, either the **traceRouteTestFailed** or **traceRouteTestCompleted** trap is generated.

RELATED DOCUMENTATION

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747
Monitoring a Running Traceroute Test | 749
SNMP Remote Operations Overview | 734
Starting a Traceroute Test | 747
Gathering Traceroute Test Results | 754
Stopping a Traceroute Test | 756
Interpreting Traceroute Variables | 756

Gathering Traceroute Test Results

You can either poll traceRouteResultsOperStatus to find out when the test is complete or request that a trap be sent when the test is complete. For more information about traceResultsOperStatus, see "traceRouteResultsTable" on page 749. For more information about Traceroute MIB traps, see the Generating Traps section in "Monitoring a Running Traceroute Test" on page 749.

Statistics are calculated on a per-hop basis and then stored in traceRouteHopsTable. They include the following for each hop:

- traceRouteHopsIpTgtAddressType—Address type of host at this hop
- traceRouteHopsIpTgtAddress—Address of host at this hop
- traceRouteHopsMinRtt—Minimum round-trip time
- traceRouteHopsMaxRtt—Maximum round-trip time
- traceRouteHopsAverageRtt—Average round-trip time
- traceRouteHopsRttSumOfSquares—Sum of squares of round-trip times
- traceRouteHopsSentProbes—Number of attempts to send probes
- traceRouteHopsProbeResponses—Number of responses received
- traceRouteHopsLastGoodProbe—Timestamp of last response

You can also consult traceRouteProbeHistoryTable for more detailed information about each probe. The index used for traceRouteProbeHistoryTable starts at 1, goes to 0xFFFFFFFF, and wraps to 1 again.

For example, assume the following:

- traceRouteCtlMaxRows is 10.
- traceRouteCtlProbesPerHop is 5.

- There are eight hops to the target (the target being number eight).
- Each probe sent results in a response from a host (the number of probes sent is not limited by traceRouteCtlMaxFailures).

In this test, 40 probes are sent. At the end of the test, traceRouteProbeHistoryTable would have a history of probes like those in Table 59 on page 755.

Table 59: traceRouteProbeHistoryTable

HistoryIndex	HistoryHopIndex	HistoryProbeIndex
31	7	1
32	7	2
33	7	3
34	7	4
35	7	5
36	8	1
37	8	2
38	8	3
39	8	4
40	8	5

RELATED DOCUMENTATION

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | **747**

Monitoring a Running Traceroute Test | **749**

SNMP Remote Operations Overview | **734**

Starting a Traceroute Test | **747**

Monitoring Traceroute Test Completion | **753**

Stopping a Traceroute Test | **756**

Interpreting Traceroute Variables | **756**

Stopping a Traceroute Test

To stop an active test, set **traceRouteCtlAdminStatus** to **disabled**. To stop a test and remove its **traceRouteCtlEntry**, **traceRouteResultsEntry**, **traceRouteProbeHistoryEntry**, and **traceRouteProbeHistoryEntry** objects from the MIB, set **traceRouteCtlRowStatus** to **destroy**.

RELATED DOCUMENTATION

- Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747
- Monitoring a Running Traceroute Test | 749
- SNMP Remote Operations Overview | 734
- Starting a Traceroute Test | 747
- Monitoring Traceroute Test Completion | 753
- Gathering Traceroute Test Results | 754
- Interpreting Traceroute Variables | 756

Interpreting Traceroute Variables

This topic contains information about the ranges for the following variables that are not explicitly specified in the Traceroute MIB:

- **traceRouteCtlMaxRows**—The maximum value for **traceRouteCtlMaxRows** is 2550. This represents the maximum TTL (255) multiplied by the maximum for **traceRouteCtlProbesPerHop** (10). Therefore, the **traceRouteProbeHistoryTable** accommodates one complete test at the maximum values for one **traceRouteCtlEntry**. Usually, the maximum values are not used and the **traceRouteProbeHistoryTable** is able to accommodate the complete history for many tests for the same **traceRouteCtlEntry**.
- **traceRouteMaxConcurrentRequests**—The maximum value is 50. If a test is running, it has one outstanding probe. **traceRouteMaxConcurrentRequests** represents the maximum number of traceroute tests that have **traceRouteResultsOperStatus** with a value of **enabled**. Any attempt to start a test with **traceRouteMaxConcurrentRequests** tests running will result in the creation of one probe with **traceRouteProbeHistoryStatus** set to **maxConcurrentLimitReached** and that test will end immediately.
- **traceRouteCtlTable**—The maximum number of entries allowed in this table is 100. Any attempt to create a 101st entry will result in a **BAD_VALUE** message for SNMPv1 and a **RESOURCE_UNAVAILABLE** message for SNMPv2.

RELATED DOCUMENTATION

- Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS | 747
- Monitoring a Running Traceroute Test | 749
- SNMP Remote Operations Overview | 734
- Starting a Traceroute Test | 747
- Monitoring Traceroute Test Completion | 753
- Gathering Traceroute Test Results | 754
- Stopping a Traceroute Test | 756

CHAPTER 18

Tracing SNMP Activity

IN THIS CHAPTER

- Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS | **758**
- Tracing SNMP Activity on a Device Running Junos OS | **766**
- Example: Tracing SNMP Activity | **770**
- Configure the Certificate Expiration Trap | **770**
- Enable Peer Down and IPsec Tunnel Down Traps | **772**

Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS

IN THIS SECTION

- Checking for MIB Objects Registered with the snmpd | **758**
- Tracking SNMP Activity | **760**
- Monitoring SNMP Statistics | **762**
- Checking CPU Utilization | **764**
- Checking Kernel and Packet Forwarding Engine Response | **765**

The following sections contain information about monitoring the SNMP activity on devices running the Junos OS and identifying problems that might impact the SNMP performance on devices running Junos OS:

Checking for MIB Objects Registered with the snmpd

For the SNMP process to be able to access data related to a MIB object, the MIB object must be registered with the snmpd. When an SNMP subagent comes online, it tries to register the associated MIB objects

with the snmpd. The snmpd maintains a mapping of the objects and the subagents with which the objects are associated. However, the registration attempt fails occasionally, and the objects remain unregistered with the snmpd until the next time the subagent restarts and successfully registers the objects.

When a network management system polls for data related to objects that are not registered with the snmpd, the snmpd returns either a **noSuchName** error (for SNMPv1 objects) or a **noSuchObject** error (for SNMPv2 objects).

You can use the following commands to check for MIB objects that are registered with the snmpd:

- **show snmp registered-objects**—Creates a **/var/log/snmp_reg_objs** file that contains the list of registered objects and their mapping to various subagents.
- **file show /var/log/snmp_reg_objs**—Displays the contents of the **/var/log/snmp_reg_objs** file.

The following example shows the steps for creating and displaying the **/var/log/snmp_reg_objs** file:

```
user@host> show snmp registered-objects

user@host> file show /var/log/snmp_reg_objs

------------------------------------------------------------
 Registered MIB Objects
 root_name =
------------------------------------------------------------
.1.2.840.10006.300.43.1.1.1.1.2 (dot3adAggMACAddress) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.3 (dot3adAggActorSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.4 (dot3adAggActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.5 (dot3adAggAggregateOrIndividual) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.6 (dot3adAggActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.7 (dot3adAggActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.8 (dot3adAggPartnerSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.9 (dot3adAggPartnerSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.10 (dot3adAggPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.11 (dot3adAggCollectorMaxDelay) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.2.1.1 (dot3adAggPortListPorts) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.2 (dot3adAggPortActorSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.3 (dot3adAggPortActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.4 (dot3adAggPortActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.5 (dot3adAggPortActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.6 (dot3adAggPortPartnerAdminSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.7 (dot3adAggPortPartnerOperSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.8 (dot3adAggPortPartnerAdminSystemID)
```

```
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.9 (dot3adAggPortPartnerOperSystemID)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.10 (dot3adAggPortPartnerAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.11 (dot3adAggPortPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.12 (dot3adAggPortSelectedAggID) (/var/run/mib2d-11)
---(more)---
```

NOTE: The **/var/log/snmp_reg_objs** file contains only those objects that are associated with the Junos OS processes that are up and running and registered with the snmpd, at the time of executing the **show snmp registered-objects** command. If a MIB object related to a Junos OS process that is up and running is not shown in the list of registered objects, you might want to restart the software process to retry object registration with the snmpd.

Tracking SNMP Activity

SNMP tracing operations track activity of SNMP agents and record the information in log files. The logged event descriptions provide detailed information to help you solve problems faster. By default, Junos OS does not trace any SNMP activity. To enable tracking of SNMP activities on a device running Junos OS, include the **traceoptions** statement at the **[edit snmp]** hierarchy level.

A sample **traceoptions** configuration might look like:

```
[edit snmp]
set traceoptions flag all;
```

When the **traceoptions flag all** statement is included at the **[edit snmp]** hierarchy level, the following log files are created:

- snmpd
- mib2d
- rmopd

You can use the **show log *log-filename*** operational mode command to view the contents of the log file. In the snmpd log file (see the following example), a sequence of **>>>** represents an incoming packet, whereas a sequence of **<<<** represents an outgoing packet. Note that the request response pair might not follow any sequence if there are multiple network management systems polling the device at the same time. You can use the source and request ID combinations to match requests and responses. However, note that no

response log is created in the log file if the SNMP master agent or the SNMP subagent has not responded to a request.

A careful analysis of the request-response time can help you identify and understand delayed responses.

Reviewing a Log File

The following example shows the output for the **show log snmpd** command:

`user@host>` **show log snmpd**

```
Apr 12 06:40:03 snmpd[7ee783df] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Apr 12 06:40:03 snmpd[7ee783df] >>> Get-Bulk-Request
Apr 12 06:40:03 snmpd[7ee783df] >>>  Source:      10.209.63.42
Apr 12 06:40:03 snmpd[7ee783df] >>>  Destination: 10.209.2.242
Apr 12 06:40:03 snmpd[7ee783df] >>>  Version:     SNMPv2
Apr 12 06:40:03 snmpd[7ee783df] >>>  Request_id:  0x7ee783df
Apr 12 06:40:03 snmpd[7ee783df] >>>  Community:   public
Apr 12 06:40:03 snmpd[7ee783df] >>>  Non-repeaters:   0
Apr 12 06:40:03 snmpd[7ee783df] >>>  Max-repetitions: 10
Apr 12 06:40:03 snmpd[7ee783df] >>>   OID  : jnxContentsType.6.1.2.0
Apr 12 06:40:03 snmpd[7ee783df] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Apr 12 06:40:03 snmpd[7ee783df]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Apr 12 06:40:03 snmpd[7ee783df]  <<< Get-Response
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Source:      10.209.63.42
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Destination: 10.209.2.242
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Version:     SNMPv2
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Request_id:  0x7ee783df
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Community:   public
Apr 12 06:40:03 snmpd[7ee783df]  <<<  Error:       status=0 / vb_index=0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.7.1.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iFPC.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.7.1.1.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxChassisTempSensor.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.7.2.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iFPC.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.7.2.1.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxChassisTempSensor.0
```

```
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.9.1.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iRE.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.9.1.1.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxPCMCIACard.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.9.2.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iRE.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.9.2.1.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxPCMCIACard.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.12.1.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iHCM.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<
Apr 12 06:40:03 snmpd[7ee783df]  <<<   OID  : jnxContentsType.12.2.0.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<   type : Object
Apr 12 06:40:03 snmpd[7ee783df]  <<<   value: jnxM10iHCM.0
Apr 12 06:40:03 snmpd[7ee783df]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Apr 12 06:40:03 snmpd[7ee783e0] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Apr 12 06:40:03 snmpd[7ee783e0] >>> Get-Bulk-Request
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Source:      10.209.63.42
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Destination: 10.209.2.242
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Version:     SNMPv2
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Request_id:  0x7ee783e0
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Community:   public
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Non-repeaters:   0
Apr 12 06:40:03 snmpd[7ee783e0] >>>  Max-repetitions: 10
Apr 12 06:40:03 snmpd[7ee783e0] >>>   OID  : jnxContentsType.12.2.0.0
Apr 12 06:40:03 snmpd[7ee783e0] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
.....
.....
```

Monitoring SNMP Statistics

The **show snmp statistics extensive** operational mode command provides you with an option to review SNMP traffic, including traps, on a device. Output for the **show snmp statistics extensive** command shows

real-time values and can be used to monitor values such as throttle drops, currently active, max active, not found, time out, max latency, current queued, total queued, and overflows. You can identify slowness in SNMP responses by monitoring the currently active count, because a constant increase in the currently active count is directly linked to slow or no response to SNMP requests.

Sample Output for the show snmp statistics extensive Command

`user@host>` **show snmp statistics extensive**

```
SNMP statistics:
 Input:
   Packets: 226656, Bad versions: 0, Bad community names: 0,
   Bad community uses: 0, ASN parse errors: 0,
   Too bigs: 0, No such names: 0, Bad values: 0,
   Read onlys: 0, General errors: 0,
   Total request varbinds: 1967606, Total set varbinds: 0,
   Get requests: 18478, Get nexts: 75794, Set requests: 0,
   Get responses: 0, Traps: 0,
   Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
   Throttle drops: 27084, Duplicate request drops: 0
 V3 Input:
   Unknown security models: 0, Invalid messages: 0
   Unknown pdu handlers: 0, Unavailable contexts: 0
   Unknown contexts: 0, Unsupported security levels: 0
   Not in time windows: 0, Unknown user names: 0
   Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
 Output:
   Packets: 226537, Too bigs: 0, No such names: 0,
   Bad values: 0, General errors: 0,
   Get requests: 0, Get nexts: 0, Set requests: 0,
   Get responses: 226155, Traps: 382
 SA Control Blocks:
   Total: 222984, Currently Active: 501, Max Active: 501,
   Not found: 0, Timed Out: 0, Max Latency: 25
 SA Registration:
   Registers: 0, Deregisters: 0, Removes: 0
 Trap Queue Stats:
   Current queued: 0, Total queued: 0, Discards: 0, Overflows: 0
 Trap Throttle Stats:
   Current throttled: 0, Throttles needed: 0
 Snmp Set Stats:
   Commit pending failures: 0, Config lock failures: 0
   Rpc failures: 0, Journal write failures: 0
   Mgd connect failures: 0, General commit failures: 0
```

Checking CPU Utilization

High CPU usage of the software processes that are being queried, such as snmpd or mib2d, is another factor that can lead to slow response or no response. You can use the **show system processes extensive** operational mode command to check the CPU usage levels of the Junos OS processes.

Sample Output of show system processes extensive Command

`user@host>` **show system processes extensive**

```
last pid:  1415;  load averages:  0.00,  0.00,  0.00  up 0+02:20:54    10:26:25
117 processes: 2 running, 98 sleeping, 17 waiting

Mem: 180M Active, 54M Inact, 39M Wired, 195M Cache, 69M Buf, 272M Free
Swap: 1536M Total, 1536M Free


  PID USERNAME  THR PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
   11 root        1 171   52     0K    12K RUN    132:09 95.21% idle
 1184 root        1  97    0 35580K  9324K select   4:16  1.61% chassisd
  177 root        1  -8    0     0K    12K mdwait   0:51  0.00% md7
  119 root        1  -8    0     0K    12K mdwait   0:20  0.00% md4
   13 root        1 -20 -139     0K    12K WAIT     0:16  0.00% swi7: clock sio
 1373 root        1  96    0 15008K 12712K select   0:09  0.00% snmpd
 1371 root        1  96    0  9520K  5032K select   0:08  0.00% jdiameterd
   12 root        1 -40 -159     0K    12K WAIT     0:07  0.00% swi2: net
 1375 root        2  96    0 15016K  5812K select   0:06  0.00% pfed
   49 root        1  -8    0     0K    12K mdwait   0:05  0.00% md0
 1345 root        1  96    0 10088K  4480K select   0:05  0.00% l2ald
 1181 root        1  96    0  1608K   908K select   0:05  0.00% bslockd
   23 root        1 -68 -187     0K    12K WAIT     0:04  0.00% irq10: fxp1
   30 root        1 171   52     0K    12K pgzero   0:04  0.00% pagezero
 1344 root        1   4    0 39704K 11444K kqread   0:03  0.00% rpd
1205 root        1  96    0  3152K   912K select   0:03  0.00% license-check
 1372 root        1  96    0 28364K  6696K select   0:03  0.00% dcd
 1374 root        1  96    0 11764K  7632K select   0:02  0.00% mib2d
 1405 user     1  96    0 15892K 11132K select   0:02  0.00% cli
  139 root        1  -8    0     0K    12K mdwait   0:02  0.00% md5
   22 root        1 -80 -199     0K    12K WAIT     0:02  0.00% irq9: cbb1 fxp0
 1185 root        1  96    0  4472K  2036K select   0:02  0.00% alarmd
    4 root        1  -8    0     0K    12K -        0:02  0.00% g_down
    3 root        1  -8    0     0K    12K -        0:02  0.00% g_up
   43 root        1 -16    0     0K    12K psleep   0:02  0.00% vmkmemdaemon
 1377 root        1  96    0  3776K  2256K select   0:01  0.00% irsd
   48 root        1 -16    0     0K    12K -        0:01  0.00% schedcpu
```

```
   99 root        1  -8    0     0K    12K mdwait   0:01  0.00% md3
  953 root        1  96    0  4168K  2428K select   0:01  0.00% eventd
 1364 root        1  96    0  4872K  2808K select   0:01  0.00% cfmd
   15 root        1 -16    0     0K    12K -        0:01  0.00% yarrow
 1350 root        1  96    0 31580K  7248K select   0:01  0.00% cosd
 1378 root        1  96    0 19776K  6292K select   0:01  0.00% lpdfd

...
```

Checking Kernel and Packet Forwarding Engine Response

As mentioned in "Understanding SNMP Implementation in Junos OS" on page 389, some SNMP MIB data are maintained by the kernel or Packet Forwarding Engine. For such data to be available for the network management system, the kernel has to provide the required information to the SNMP subagent in mib2d. A slow response from the kernel can cause a delay in mib2d returning the data to the network management system. Junos OS adds an entry in the mib2d log file every time that an interface takes more than 10,000 microseconds to respond to a request for interface statistics. You can use the **show log *log-filename* | grep "kernel response time"** command to find out the response time taken by the kernel.

Checking the Kernel Response Time

`user@host>` **show log mib2d | grep "kernel response time"**

```
Aug 17 22:39:37  == kernel response time for
COS_IPVPN_DEFAULT_OUTPUT-t1-7/3/0:10:27.0-o: 9.126471 sec, range
(0.000007, 11.000806)

Aug 17 22:39:53  == kernel response time for
COS_IPVPN_DEFAULT_INPUT-t1-7/2/0:5:15.0-i: 5.387321 sec, range
(0.000007, 11.000806)

Aug 17 22:39:53  == kernel response time for ct1-6/1/0:9:15: 0.695406
sec, range (0.000007, 11.000806)

Aug 17 22:40:04  == kernel response time for t1-6/3/0:6:19: 1.878542
sec, range (0.000007, 11.000806)

Aug 17 22:40:22  == kernel response time for lsq-7/0/0: 2.556592 sec,
range (0.000007, 11.000806)
```

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | 389
- Best Practices for Configuring SNMP | 558
- Optimizing the Network Management System Configuration for the Best Results | 555
- Configuring Options on Managed Devices for Better SNMP Response Time | 556
- Managing Traps and Informs | 432
- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage | 643

Tracing SNMP Activity on a Device Running Junos OS

IN THIS SECTION

- Configuring the Number and Size of SNMP Log Files | 767
- Configuring Access to the Log File | 767
- Configuring a Regular Expression for Lines to Be Logged | 768
- Configuring the Trace Operations | 768

SNMP tracing operations track activity for SNMP agents and record the information in log files. The logged error descriptions provide detailed information to help you solve problems faster.

By default, Junos OS does not trace any SNMP activity. If you include the **traceoptions** statement at the **[edit snmp]** hierarchy level, the default tracing behavior is:

- Important activities are logged in files located in the **/var/log** directory. Each log is named after the SNMP agent that generates it. Currently, the following log files are created in the **/var/log** directory when the **traceoptions** statement is used:
  - chassisd
  - craftd
  - ilmid
  - mib2d
  - rmopd
  - serviced
  - snmpd

- When a trace file named ***filename*** reaches its maximum size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. (For more information about how log files are created, see the System Log Explorer.)
- Log files can be accessed only by the user who configured the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
traceoptions {
    file <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    memory-trace;
    no-remote-trace;
    no-default-memory-trace;
}
```

These statements are described in the following sections:

Configuring the Number and Size of SNMP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until there are three trace files. Then the oldest trace file (***filename*.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename*.0**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0** is renamed ***filename*.1** and ***filename*** is renamed ***filename*.0**. This process repeats until there are 20 trace files. Then the oldest file (***filename*.19**) is overwritten by the newest file (***filename*.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configured the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged activities.

You can refine the output by including the **match** statement at the **[edit snmp traceoptions file *filename*]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit snmp traceoptions]
file filename match regular-expression;
```

Configuring the Trace Operations

By default, only important activities are logged. You can specify which trace operations are to be logged by including the following **flag** statement (with one or more tracing flags) at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
flag {
    all;
    configuration;
    database;
    events;
    general;
    interface-stats;
    nonvolatile-sets;
    pdu;
    policy;
    protocol-timeouts;
    routing-socket;
```

```
    server;
    subagent;
    timer;
    varbind-error;
}
```

Table 60 on page 769 describes the meaning of the SNMP tracing flags.

Table 60: SNMP Tracing Flags

Flag	Description	Default Setting
all	Log all operations.	Off
configuration	Log reading of the configuration at the **[edit snmp]** hierarchy level.	Off
database	Log events involving storage and retrieval in the events database.	Off
events	Log important events.	Off
general	Log general events.	Off
interface-stats	Log physical and logical interface statistics.	Off
nonvolatile-set	Log nonvolatile SNMP set request handling.	Off
pdu	Log SNMP request and response packets.	Off
policy	Log policy processing.	Off
protocol-timeouts	Log SNMP response timeouts.	Off
routing-socket	Log routing socket calls.	Off
server	Log communication with processes that are generating events.	Off
subagent	Log subagent restarts.	Off
timer	Log internal timer events.	Off
varbind-error	Log variable binding errors.	Off

To display the end of the log for an agent, issue the **show log *agentd* | last** operational mode command:

```
[edit]
user@host# run show log agentd | last
```

where ***agent*** is the name of an SNMP agent.

RELATED DOCUMENTATION

Example: Tracing SNMP Activity | 770
Configuring SNMP | 550

Example: Tracing SNMP Activity

Trace information about SNMP packets:

```
[edit]
snmp {
    traceoptions {
        file size 10k files 5;
        flag pdu;
        flag protocol-timeouts;
        flag varbind-error;
    }
}
```

RELATED DOCUMENTATION

Tracing SNMP Activity on a Device Running Junos OS | 766
Configuration Statements at the [edit snmp] Hierarchy Level | 545

Configure the Certificate Expiration Trap

This topic shows how to configure certificate expiration trap and configure the number of days before to generate the trap.

Before you begin:

- Understand how certificates works on VPN. Read Understanding Certificate Chains.

1. Configure the number of days before to generate the trap for all certificates.

   ```
   user@host# set security pki trap all-certificates number-of-days
   ```

2. Configure the number of days before to generate the trap for CA certificate.

   ```
   user@host# set security pki trap ca-identity ca-profile-name number-of-days
   ```

3. Configure the number of days before to generate the trap for local certificate.

   ```
   user@host# set security pki trap certificate-idcertificate-id-name number-of-days
   ```

4. Confirm your configuration by entering the **show security pki trap** command.

   ```
   user@host# show security pki trap
   certificate-id crt_spk1 {
       30;
   }
   ca-identity Root-CA {
       30;
   }
   all-certificates {
       30;
   }
   ```

RELATED DOCUMENTATION

Enable Peer Down and IPsec Tunnel Down Traps | 772

trap (Security PKI) | 2258

show security ipsec statistics

Enable Peer Down and IPsec Tunnel Down Traps

This topic shows how to enable **peer-down** and **ipsec-tunnel-down** traps.

1. Enable the IKE trap peer down. Trap gets generated when the peer is down.

```
user@host# set security ike trap peer-down
```

2. Enable the IKE trap IPsec tunnel down. Trap gets generated when the peer is up and the IPsec SA is down.

```
user@host# set security ike trap ipsec-tunnel-down
```

3. Confirm your configuration by entering the **show security ike trap** command.

```
user@host# show security ike trap
ipsec-tunnel-down;
peer-down;
```

RELATED DOCUMENTATION

Configure the Certificate Expiration Trap | 770

trap (Security PKI) | 2258

show security ipsec statistics

5

PART

Remote Monitoring (RMON) with SNMP Alarms and Events

RMON Overview | **774**

Using RMON to Monitor Network Service Quality | **802**

Health Monitoring with SNMP | **831**

CHAPTER 19

RMON Overview

IN THIS CHAPTER

- Understanding RMON | 774
- Understanding RMON Alarms | 777
- Understanding RMON Events | 779
- Understanding RMON Alarms and Events Configuration | 780
- RMON MIB Event, Alarm, Log, and History Control Tables | 781
- Minimum RMON Alarm and Event Entry Configuration | 783
- Configuring an RMON Alarm Entry and Its Attributes | 784
- Configuring an RMON Event Entry and Its Attributes | 789
- Example: Configuring an RMON Alarm and Event Entry | 790
- Configuring RMON History Sampling | 791
- Using alarmTable to Monitor MIB Objects | 793
- Using eventTable to Log Alarms | 798

Understanding RMON

IN THIS SECTION

- RMON Overview | 774
- Alarm Thresholds and Events | 775

RMON Overview

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds.

When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

An operational support system (OSS) or a fault-monitoring system can be used to automatically monitor events that track many different metrics, including performance, availability, faults, and environmental data. For example, an administrator might want to know when the internal temperature of a chassis has risen above a configured threshold, which might indicate that a chassis fan tray is faulty, the chassis air flow is impeded, or the facility cooling system in the vicinity of the chassis is not operating normally.

The RMON MIB also defines tables that store various statistics for Ethernet interfaces, including the **etherStatsTable** and the **etherHistoryTable**. The **etherStatsTable** contains cumulative real-time statistics for Ethernet interfaces, such as the number of unicast, multicast, and broadcast packets received on an interface. The **etherHistoryTable** maintains a historical sample of statistics for Ethernet interfaces. The control of the **etherHistoryTable**, including the interfaces to track and the sampling interval, is defined by the RMON **historyControlTable**.

To enable RMON alarms, you perform the following steps:

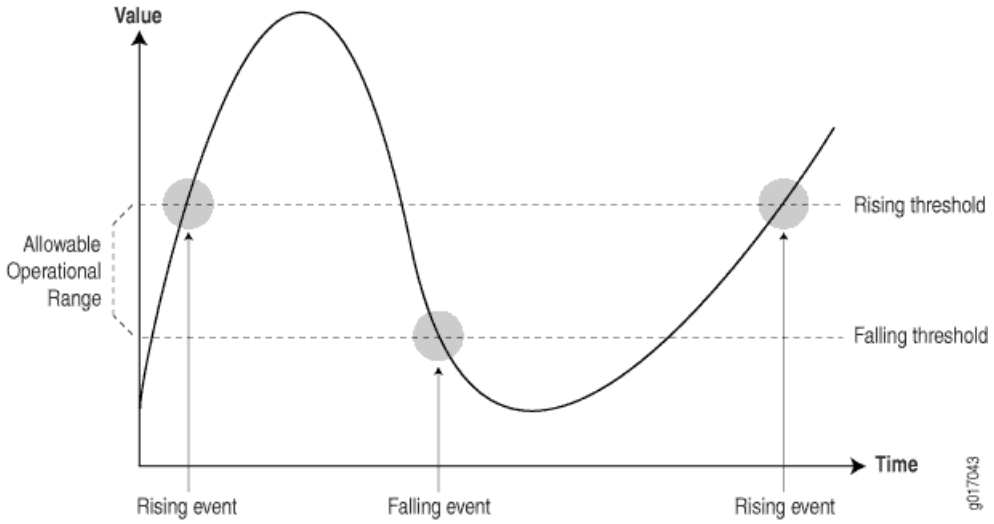
1. Configure SNMP, including trap groups. You configure SNMP at the [**edit snmp**] hierarchy level.
2. Configure rising and falling events in the **eventTable**, including the event types and trap groups. You can also configure events using the CLI at the [**edit snmp rmon event**] hierarchy level.
3. Configure alarms in the **alarmTable**, including the variables to monitor, rising and falling thresholds, the sampling types and intervals, and the corresponding events to generate when alarms occur. You can also configure alarms using the CLI at the [**edit snmp rmon alarm**] hierarchy level.

   Extensions to the **alarmTable** are defined in the Juniper Networks enterprise-specific MIB jnxRmon (mib-jnx-rmon.txt).

Alarm Thresholds and Events

By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range (see Figure 28 on page 776).

Figure 28: Setting Thresholds



Events are only generated when the alarm threshold is first crossed in any one direction rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs. This considerably reduces the quantity of events that are produced by the system, making it easier for operations staff to react when events do occur.

Before you configure remote monitoring, you should identify what variables need to be monitored and their allowable operational range. This requires some period of baselining to determine the allowable operational ranges. An initial baseline period of at least
3 months is not unusual when you first identify the operational ranges and define thresholds, but baseline monitoring should continue over the life span of each monitored variable.

RELATED DOCUMENTATION

Configuring RMON Alarms and Events | **652**

Juniper Networks Enterprise-Specific MIBs

RMON MIB Event, Alarm, Log, and History Control Tables | **781**

Understanding RMON Alarms

IN THIS SECTION

- alarmTable | 777
- jnxRmonAlarmTable | 778

An RMON alarm identifies:

- A specific MIB object that is monitored.
- The frequency of sampling.
- The method of sampling.
- The thresholds against which the monitored values are compared.

An RMON alarm can also identify a specific **eventTable** entry to be triggered when a threshold is crossed.

Configuration and operational values are defined in **alarmTable** in RFC 2819. Additional operational values are defined in Juniper Networks enterprise-specific extensions to **alarmTable** (**jnxRmonAlarmTable**).

This topic covers the following sections:

alarmTable

alarmTable in the RMON MIB allows you to monitor and poll the following:

- **alarmIndex**—The index value for **alarmTable** that identifies a specific entry.
- **alarmInterval**—The interval, in seconds, over which data is sampled and compared with the rising and falling thresholds.
- **alarmVariable**—The MIB variable that is monitored by the alarm entry.
- **alarmSampleType**—The method of sampling the selected variable and calculating the value to be compared against the thresholds.
- **alarmValue**—The value of the variable during the last sampling period. This value is compared with the rising and falling thresholds.
- **alarmStartupAlarm**—The alarm sent when the entry is first activated.
- **alarmRisingThreshold**—The upper threshold for the sampled variable.
- **alarmFallingThreshold**—The lower threshold for the sampled variable.

- **alarmRisingEventIndex**—The **eventTable** entry used when a rising threshold is crossed.
- **alarmFallingEventIndex**—The **eventTable** entry used when a falling threshold is crossed.
- **alarmStatus**—Method for adding and removing entries from the table. It can also be used to change the state of an entry to allow modifications.

> **NOTE:** If this object is not set to **valid**, the associated event alarm does not take any action.

jnxRmonAlarmTable

The **jnxRmonAlarmTable** is a Juniper Networks enterprise-specific extension to **alarmTable**. It provides additional operational information and includes the following objects:

- **jnxRmonAlarmGetFailCnt**—The number of times the internal **Get** request for the variable monitored by this entry has failed.
- **jnxRmonAlarmGetFailTime**—The value of **sysUpTime** when an internal **Get** request for the variable monitored by this entry last failed.
- **jnxRmonAlarmGetFailReason**—The reason an internal **Get** request for the variable monitored by this entry last failed.
- **jnxRmonAlarmGetOkTime**—The value of **sysUpTime** when an internal **Get** request for the variable monitored by this entry succeeded and the entry left the **getFailure** state.
- **jnxRmonAlarmState**—The current state of this RMON alarm entry.

To view the Juniper Networks enterprise-specific extensions to the RMON Events and Alarms and Event MIB, see https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-rmon.txt.

RELATED DOCUMENTATION

Understanding RMON Events | 779

Configuring an RMON Alarm Entry and Its Attributes | 784

Using alarmTable to Monitor MIB Objects | 793

Understanding RMON Events

IN THIS SECTION

- eventTable | 779

An RMON event allows you to log the crossing of thresholds of other MIB objects. It is defined in **eventTable** for the RMON MIB.

This section covers the following topics:

eventTable

eventTable contains the following objects:

- **eventIndex**—An index that uniquely identifies an entry in **eventTable**. Each entry defines one event that is generated when the appropriate conditions occur.
- **eventDescription**—A comment describing the event entry.
- **eventType**—Type of notification that the probe makes about this event.
- **eventCommunity**—Trap group used if an SNMP trap is to be sent. If **eventCommunity** is not configured, a trap is sent to each trap group configured with the **rmon-alarm** category.
- **eventLastTimeSent**—Value of **sysUpTime** when this event entry last generated an event.
- **eventOwner**—Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.
- **eventStatus**—Status of this event entry.

> **NOTE:** If this object is not set to **valid**, no action is taken by the associated event entry. When this object is set to **valid**, all previous log entries associated with this entry (if any) are deleted.

RELATED DOCUMENTATION

Understanding RMON Alarms | 777

Configuring an RMON Event Entry and Its Attributes | 789

Understanding RMON Alarms and Events Configuration

Junos OS supports monitoring routers from remote devices. These values are measured against thresholds and trigger events when the thresholds are crossed. You configure remote monitoring (RMON) alarm and event entries to monitor the value of a MIB object.

To configure RMON alarm and event entries, you include statements at the **[edit snmp]** hierarchy level of the configuration:

```
[edit snmp]
rmon {
    alarm index {
        description text-description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        rising-event-index index;
        rising-threshold integer;
        request-type (get-next-request | get-request | walk-request);
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
}
```

RELATED DOCUMENTATION

Understanding RMON Alarms | 777

Understanding RMON Events | 779

Configuring an RMON Alarm Entry and Its Attributes | 784

Configuring an RMON Event Entry and Its Attributes | 789

RMON MIB Event, Alarm, Log, and History Control Tables

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

Table 61 on page 781 provides each field in the RMON eventTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon**] hierarchy level.

Table 61: RMON Event Table

Field	Description	Statement [edit snmp rmon]
eventDescription	Text description of this event.	**description**
eventType	Type of event (for example, log, trap, or log and trap).	**type**
eventCommunity	Trap group to which to send this event, as defined in the Junos OS configuration. (This is not the same as the SNMP community.)	**community**
eventOwner	Entity (for example, manager) that created this event.	—
eventStatus	Status of this row (for example, valid, invalid, or createRequest).	—

Table 62 on page 781 provides each field in the RMON alarmTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon**] hierarchy level.

Table 62: RMON Alarm Table

Field	Description	Statement [edit snmp rmon]
alarmStatus	Status of this row (for example, valid, invalid, or createRequest)	—
alarmInterval	Sampling period (in seconds) of the monitored variable	**interval**
alarmVariable	Object identifier (OID) and instance of the variable to be monitored	—
alarmValue	Actual value of the sampled variable	—

Table 62: RMON Alarm Table *(continued)*

Field	Description	Statement [edit snmp rmon]
alarmSampleType	Sample type (absolute or delta changes)	**sample-type**
alarmStartupAlarm	Initial alarm (rising, falling, or either)	**startup-alarm**
alarmRisingThreshold	Rising threshold against which to compare the value	**rising-threshold**
alarmFallingThreshold	Falling threshold against which to compare the value	**falling-threshold**
alarmRisingEventIndex	Index (row) of the rising event in the event table	**rising-event-index**
alarmFallingEventIndex	Index (row) of the falling event in the event table	**falling-event-index**

Table 63 on page 782 provides each field in the jnxRmon jnxRmonAlarmTable, which is an extension to the RMON alarmTable. You can troubleshoot the RMON agent, rmopd, that runs on a switch by inspecting the contents of the jnxRmonAlarmTable object.

Table 63: jnxRmon Alarm Table

Field	Description
jnxRmonAlarmGetFailCnt	Number of times the internal **Get** request for the variable failed
jnxRmonAlarmGetFailTime	Value of the sysUpTime object when the last failure occurred
jnxRmonAlarmGetFailReason	Reason why the **Get** request failed
jnxRmonAlarmGetOkTime	Value of the sysUpTime object when the variable moved out of failure state
jnxRmonAlarmState	Status of this alarm entry

Table 64 on page 783 provides each field in the RMON historyControlTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon history**] hierarchy level. The historyControlTable controls the RMON etherHistoryTable.

Table 64: RMON History Control Table

Field	Description	Statement [edit snmp rmon history]
historyControlDataSource	Identifies the source of the data for which historical data was collected.	**interface**
historyControlBucketsRequested	Requested number of discrete time intervals over which data is to be saved.	**bucket-size**
historyControlBucketsGranted	Number of discrete sampling intervals over which data is to be saved.	—
historyControlInterval	Interval, in seconds, over which the data is sampled for each bucket.	**interval**
historyControlOwner	Entity that configured this entry.	**owner**
historyControlStatus	Status of this entry.	—

RELATED DOCUMENTATION

Configuring RMON Alarms and Events | 652

Juniper Networks Enterprise-Specific MIBs

Understanding RMON | 774

Minimum RMON Alarm and Event Entry Configuration

To enable RMON on the router, you must configure an alarm entry and an event entry. To do this, include the following statements at the **[edit snmp rmon]** hierarchy level:

```
[edit snmp rmon]
alarm index {
    rising-event-index index;
    rising-threshold integer;
    sample-type type;
    variable oid-variable;
}
```

```
event index;
```

RELATED DOCUMENTATION

- Understanding RMON Alarms and Events Configuration | 780
- Configuring an RMON Alarm Entry and Its Attributes | 784
- Configuring an RMON Event Entry and Its Attributes | 789

Configuring an RMON Alarm Entry and Its Attributes

IN THIS SECTION

- Configuring the Alarm Entry | 784
- Configuring the Description | 785
- Configuring the Falling Event Index or Rising Event Index | 785
- Configuring the Falling Threshold or Rising Threshold | 786
- Configuring the Interval | 786
- Configuring the Falling Threshold Interval | 787
- Configuring the Request Type | 787
- Configuring the Sample Type | 787
- Configuring the Startup Alarm | 788
- Configuring the System Log Tag | 788
- Configuring the Variable | 789

An alarm entry monitors the value of a MIB variable. You can configure how often the value is sampled, the type of sampling to perform, and what event to trigger if a threshold is crossed.

This section discusses the following topics:

Configuring the Alarm Entry

An alarm entry monitors the value of a MIB variable. The **rising-event-index**, **rising-threshold**, **sample-type**, and **variable** statements are mandatory. All other statements are optional.

To configure the alarm entry, include the **alarm** statement and specify an index at the **[edit snmp rmon]** hierarchy level:

```
[edit snmp rmon]
alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising alarm | rising-or-falling-alarm);
    variable oid-variable;
}
```

index is an integer that identifies an alarm or event entry.

Configuring the Description

The description is a text string that identifies the alarm entry.

To configure the description, include the **description** statement and a description of the alarm entry at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
description description;
```

Configuring the Falling Event Index or Rising Event Index

The falling event index identifies the event entry that is triggered when a falling threshold is crossed. The rising event index identifies the event entry that is triggered when a rising threshold is crossed.

To configure the falling event index or rising event index, include the **falling-event-index** or **rising-event-index** statement and specify an index at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
falling-event-index index;
rising-event-index index;
```

index can be from 0 through 65,535. The default for both the falling and rising event index is 0.

Configuring the Falling Threshold or Rising Threshold

The falling threshold is the lower threshold for the monitored variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated startup alarm is equal to **falling-alarm** or **rising-or-falling-alarm**. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising threshold. You must specify the falling threshold as an integer. Its default is 20 percent less than the rising threshold.

By default, the rising threshold is 0. The rising threshold is the upper threshold for the monitored variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold, and the associated **startup-alarm** is equal to **rising-alarm** or **rising-or-falling-alarm**. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. You must specify the rising threshold as an integer.

To configure the falling threshold or rising threshold, include the **falling-threshold** or **rising-threshold** statement at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
falling-threshold integer;
rising-threshold integer;
```

integer can be a value from -2,147,483,647 through 2,147,483,647.

Configuring the Interval

The interval represents the period of time, in seconds, over which the monitored variable is sampled and compared with the rising and falling thresholds.

To configure the interval, include the **interval** statement and specify the number of seconds at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
interval seconds;
```

seconds can be a value from 1 through 2,147,483,647. The default is 60 seconds.

Configuring the Falling Threshold Interval

The falling threshold interval represents the interval between samples when the rising threshold is crossed. Once the alarm crosses the falling threshold, the regular sampling interval is used.

> **NOTE:** You cannot configure the falling threshold interval for alarms that have the request type set to **walk-request**.

To configure the falling threshold interval, include the **falling-threshold interval** statement at the **[edit snmp rmon alarm *index*]** hierarchy level and specify the number of seconds:

```
[edit snmp rmon alarm index]
falling-threshold-interval seconds;
```

seconds can be a value from 1 through 2,147,483,647. The default is 60 seconds.

Configuring the Request Type

By default an RMON alarm can monitor only one object instance (as specified in the configuration). You can configure a **request-type** statement to extend the scope of the RMON alarm to include all object instances belonging to a MIB branch or to include the next object instance after the instance specified in the configuration.

To configure the request type, include the **request-type** statement at the **[edit snmp rmon alarm *index*]** hierarchy level and specify **get-next-request**, **get-request**, or **walk-request**:

```
[edit snmp rmon alarm index]
request-type (get-next-request | get-request | walk-request);
```

walk extends the RMON alarm configuration to all object instances belonging to a MIB branch. **next** extends the RMON alarm configuration to include the next object instance after the instance specified in the configuration.

Configuring the Sample Type

The sample type identifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is **absolute-value**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is **delta-value**, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.

To configure the sample type, include the **sample-type** statement and specify the type of sample at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
sample-type (absolute-value | delta-value);
```

- **absolute-value**—Actual value of the selected variable is compared against the thresholds.
- **delta-value**—Difference between samples of the selected variable is compared against the thresholds.

Configuring the Startup Alarm

The startup alarm identifies the type of alarm that can be sent when this entry is first activated. You can specify it as **falling-alarm**, **rising-alarm**, or **rising-or-falling-alarm**.

To configure the startup alarm, include the **startup-alarm** statement and specify the type of alarm at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

- **falling-alarm**—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.
- **rising-alarm**—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.
- **rising-or-falling-alarm**—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

The default is **rising-or-falling-alarm**.

Configuring the System Log Tag

The **syslog-subtag** statement specifies the tag to be added to the system log message. You can specify a string of not more than 80 uppercase characters as the system log tag.

To configure the system log tag, include the **syslog-subtag** statement at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
syslog-subtag syslog-subtag;
```

Configuring the Variable

The variable identifies the MIB object that is being monitored.

To configure the variable, include the **variable** statement and specify the object identifier or object name at the **[edit snmp rmon alarm *index*]** hierarchy level:

```
[edit snmp rmon alarm index]
variable oid-variable;
```

oid-variable is a dotted decimal (for example, **1.3.6.1.2.1.2.1.2.2.1.10.1**) or MIB object name (for example, **ifInOctets.1**).

SEE ALSO

- Understanding RMON Alarms and Events Configuration | **780**
- Understanding RMON Alarms | **777**
- Understanding RMON Events | **779**
- Configuring an RMON Event Entry and Its Attributes | **789**
- Example: Configuring an RMON Alarm and Event Entry | **790**

Configuring an RMON Event Entry and Its Attributes

An event entry generates a notification for an alarm entry when its rising or falling threshold is crossed. You can configure the type of notification that is generated. To configure the event entry, include the **event** statement at the **[edit snmp rmon]** hierarchy level. All statements except the **event** statement are optional.

```
[edit snmp rmon]
event index {
    community community-name;
    description description;
    type type;
}
```

index identifies an entry event.

community-name is the trap group that is used when generating a trap. If that trap group has the **rmon-alarm** trap category configured, a trap is sent to all the targets configured for that trap group. The community

string in the trap matches the name of the trap group. If nothing is configured, all the trap groups are examined, and traps are sent using each group with the **rmon-alarm** category set.

description is a text string that identifies the entry.

The ***type*** variable of an event entry specifies where the event is to be logged. You can specify the type as one of the following:

- **log**—Adds the event entry to the **logTable**.
- **log-and-trap**—Sends an SNMP trap and creates a log entry.
- **none**—Sends no notification.
- **snmptrap**—Sends an SNMP trap.

The default for the event entry type is **log-and-trap**.

RELATED DOCUMENTATION

Understanding RMON Alarms and Events Configuration | **780**

Understanding RMON Alarms | **777**

Understanding RMON Events | **779**

Configuring an RMON Alarm Entry and Its Attributes | **784**

Example: Configuring an RMON Alarm and Event Entry | **790**

Example: Configuring an RMON Alarm and Event Entry

Configure an RMON alarm and event entry:

```
[edit snmp]
rmon {
   alarm 100 {
      description “input traffic on fxp0”;
      falling-event-index 100;
      falling-threshold 10000;
      interval 60;
      rising-event-index 100;
      rising-threshold 100000;
      sample-type delta-value;
      startup-alarm rising-or-falling-alarm;
      variable ifInOctets.1;
```

```
    }
    event 100 {
        community bedrock;
        description” emergency events”;
        type log-and-trap;
    }
}
```

RELATED DOCUMENTATION

Understanding RMON Alarms and Events Configuration | 780
Configuring an RMON Alarm Entry and Its Attributes | 784
Configuring an RMON Event Entry and Its Attributes | 789

Configuring RMON History Sampling

IN THIS SECTION

Configuring RMON History Sampling Collection | 791
Viewing and Clearing RMON History Statistics | 792

The Junos OS supports the history control group (**etherHistoryTable**) of the *Remote Network Monitoring* (RMON) MIB (RFC 2819). The history control tables record statistical samples from an Ethernet network and store them for later retrieval.

To configure RMON history sampling and view or clear collected statistics using the Junos OS CLI, perform the following tasks:

Configuring RMON History Sampling Collection

Use the **history** statement at the **[edit snmp rmon]** hierarchy level to configure RMON history sampling collection parameters. The following parameters are required:

- History index: The history entry is identified by an integer history index value (**historyControlIndex** MIB field) specified when you configure this statement, which is used to display or clear collected results later.
- Interface: The interface to monitor for the specified history index. Only one interface can be associated with a particular RMON history index.

In addition to the required parameters, you can specify a custom sampling **interval** (in seconds) and the sampling **bucket-size** (number of discrete samples to be collected in a given interval).

```
[edit snmp]
```

```
user@switch# set rmon history history-index interface interface-name
```

```
user@switch# set rmon history history-index interval seconds
```

```
user@switch# set rmon history history-index bucket-size number
```

An optional tag (**owner**) associated with the history index can also be assigned to the collection.

Viewing and Clearing RMON History Statistics

Use the **show snmp rmon history** command to display collected RMON history table entries. You can also use the **show snmp mib walk** command to view RMON history table field samples.

The following sample RMON configuration sets up a history table sampling for interface xe-0/0/20.0 using a history index value of 1:

```
user@switch# show snmp | display set
```

```
set snmp rmon history 1 interface xe-0/0/20.0
set snmp rmon history 1 bucket-size 1000
set snmp rmon history 1 interval 5
set snmp rmon history 1 owner test
```

Using the **show snmp mib walk** command, you can see **etherHistoryPkts** field statistics collected for history index 1:

```
user@switch> show snmp mib walk etherHistoryPkts
```

```
etherHistoryPkts.1.1 = 0
<...>
etherHistoryPkts.1.148 = 10
etherHistoryPkts.1.149 = 14
```

To clear collected RMON history statistics, use the **clear snmp history** command. After clearing samples collected up to that point, collection continues again at the configured interval, and new samples are recorded. This command has options to clear collected samples of a particular configured history index or to clear all samples from all configured indices.

For example, the following command clears collected RMON history samples for history control index 1 configured above:

```
user@switch> clear snmp history 1

Samples collected are cleared.

user@switch> show snmp mib walk etherHistoryPkts | no-more

user@switch> show snmp mib walk etherHistoryPkts | no-more

etherHistoryPkts.1.1 = 0
```

RELATED DOCUMENTATION

RMON MIB Event, Alarm, Log, and History Control Tables | 781

Using alarmTable to Monitor MIB Objects

IN THIS SECTION

- Creating an Alarm Entry | 794
- Configuring the Alarm MIB Objects | 794
- Activating a New Row in alarmTable | 797
- Modifying an Active Row in alarmTable | 797
- Deactivating a Row in alarmTable | 797

To use alarmTable to monitor a MIB object, perform the following tasks:

Creating an Alarm Entry

To create an alarm entry, first create a new row in alarmTable using the alarmStatus object. For example, create alarm #1 using the UCD command-line utilities:

```
snmpset -Os -v2c router community alarmStatus.1 i createRequest
```

Configuring the Alarm MIB Objects

IN THIS SECTION

- alarmInterval | **794**
- alarmVariable | **795**
- alarmSampleType | **795**
- alarmValue | **795**
- alarmStartupAlarm | **795**
- alarmRisingThreshold | **795**
- alarmFallingThreshold | **796**
- alarmOwner | **796**
- alarmRisingEventIndex | **796**
- alarmFallingEventIndex | **796**

Once you have created the new row in alarmTable, configure the following Alarm MIB objects:

> **NOTE:** Other than alarmStatus, you cannot modify any of the objects in the entry if the associated alarmStatus object is set to **valid**.

alarmInterval

The interval, in seconds, over which data is sampled and compared with the rising and falling thresholds. For example, to set **alarmInterval** for alarm #1 to 30 seconds, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmInterval.1 i 30
```

alarmVariable

The object identifier of the variable to be sampled. During a **Set** request, if the supplied variable name is not available in the selected MIB view, a badValue error is returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe changes the status of alarmVariable to invalid. For example, to identify ifInOctets.61 as the variable to be monitored, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmVariable.1 o .1.3.6.1.2.1.2.2.1.10.61
```

alarmSampleType

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds. For example, to set alarmSampleType for alarm #1 to deltaValue, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmSampleType.1 i deltaValue
```

alarmValue

The value of the variable during the last sampling period. This value is compared with the rising and falling thresholds. If the sample type is deltaValue, this value equals the difference between the samples at the beginning and end of the period. If the sample type is **absoluteValue**, this value equals the sampled value at the end of the period.

alarmStartupAlarm

An alarm that is sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to **risingThreshold**, and **alarmStartupAlarm** is equal to **risingAlarm** or **risingOrFallingAlarm**, then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to **fallingThreshold** and **alarmStartupAlarm** is equal to **fallingAlarm** or **risingOrFallingAlarm**, then a single falling alarm is generated. For example, to set **alarmStartupAlarm** for alarm #1 to **risingOrFallingAlarm**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStartupAlarm.1 i risingOrFallingAlarm
```

alarmRisingThreshold

A threshold for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal

to this threshold, and the associated **alarmStartupAlarm** is equal to **risingAlarm** or **risingOrFallingAlarm**. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches **alarmFallingThreshold**. For example, to set **alarmRisingThreshold** for alarm #1 to **100000**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmRisingThreshold.1 i 100000
```

alarmFallingThreshold

A threshold for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated **alarmStartupAlarm** is equal to **fallingAlarm** or **risingOrFallingAlarm**. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches **alarmRisingThreshold**. For example, to set **alarmFallingThreshold** for alarm #1 to **10000**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 10000
```

alarmOwner

Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.

alarmRisingEventIndex

The index of the eventEntry object that is used when a rising threshold is crossed. If there is no corresponding entry in eventTable, then no association exists. If this value is zero, no associated event is generated because zero is not a valid event index. For example, to set alarmRisingEventIndex for alarm #1 to **10**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmRisingEventIndex.1 i 10
```

alarmFallingEventIndex

The index of the eventEntry object that is used when a falling threshold is crossed. If there is no corresponding entry in eventTable, then no association exists. If this value is zero, no associated event is generated because zero is not a valid event index. For example, to set alarmFallingEventIndex for alarm #1 to **10**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingEventIndex.1 i 10
```

Activating a New Row in alarmTable

To activate a new row in alarmTable, set alarmStatus to **valid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Modifying an Active Row in alarmTable

To modify an active row, first set alarmStatus to underCreation using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i underCreation
```

Then change the row contents using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 1000
```

Finally, activate the row by setting alarmStatus to **valid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Deactivating a Row in alarmTable

To deactivate a row in alarmTable, set alarmStatus to **invalid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i invalid
```

RELATED DOCUMENTATION

- Understanding RMON Alarms | **777**
- Understanding RMON Events | **779**
- Configuring an RMON Alarm Entry and Its Attributes | **784**

Using eventTable to Log Alarms

IN THIS SECTION

- Creating an Event Entry | 798
- Configuring the MIB Objects | 798
- Activating a New Row in eventTable | 800
- Deactivating a Row in eventTable | 800

To use eventTable to log alarms, perform the following tasks:

Creating an Event Entry

The RMON eventTable controls the generation of notifications from the router. Notifications can be logs (entries to logTable and syslogs) or SNMP traps. Each event entry can be configured to generate any combination of these notifications (or no notification). When an event specifies that an SNMP trap is to be generated, the trap group that is used when sending the trap is specified by the value of the associated eventCommunity object. Consequently, the community in the trap message will match the value specified by eventCommunity. If nothing is configured for eventCommunity, a trap is sent using each trap group that has the rmon-alarm category configured.

Configuring the MIB Objects

IN THIS SECTION

- eventType | 799
- eventCommunity | 799
- eventOwner | 799
- eventDescription | 800

Once you have created the new row in eventTable, set the following objects:

NOTE: The eventType object is required. All other objects are optional.

eventType

The type of notification that the router generates when the event is triggered.

This object can be set to the following values:

- **log**—Adds the event entry to logTable.
- **log-and-trap**—Sends an SNMP trap and creates a log entry.
- **none**—Sends no notification.
- **snmptrap**—Sends an SNMP trap.

For example, to set **eventType** for event #1 to **log-and-trap**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventType.1 i log-and-trap
```

eventCommunity

The trap group that is used when generating a trap (if eventType is configured to send traps). If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of eventCommunity). If nothing is configured, traps are sent to each group with the rmon-alarm category set. For example, to set eventCommunity for event #1 to boy-elroy, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventCommunity.1 s "boy-elroy"
```

NOTE: The eventCommunity object is optional. If you do not set this object, then the field is left blank.

eventOwner

Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.

For example, to set eventOwner for event #1 to george jetson, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventOwner.1 s "george jetson"
```

> **NOTE:** The eventOwner object is optional. If you do not set this object, then the field is left blank.

eventDescription

Any text string specified by the creating management application or the command-line interface (CLI). The use of this string is application dependent.

For example, to set eventDescription for event #1 to spacelys sprockets, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventDescription.1 s "spacelys sprockets"
```

> **NOTE:** The eventDescription object is optional. If you do not set this object, then the field is left blank.

Activating a New Row in eventTable

To activate the new row in eventTable, set eventStatus to **valid** using an SNMP **Set** request such as:

```
snmpset -Os -v2c router community eventStatus.1 i valid
```

Deactivating a Row in eventTable

To deactivate a row in eventTable, set eventStatus to **invalid** using an SNMP **Set** request such as:

```
snmpset -Os -v2c router community eventStatus.1 i invalid
```

RELATED DOCUMENTATION

Understanding RMON Alarms | 777

Understanding RMON Events | 779

Configuring an RMON Event Entry and Its Attributes | 789

CHAPTER 20

Using RMON to Monitor Network Service Quality

IN THIS CHAPTER

- Understanding RMON for Monitoring Service Quality | 802
- Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806
- Defining and Measuring Network Availability | 809
- Measuring Health | 815
- Measuring Performance | 822

Understanding RMON for Monitoring Service Quality

IN THIS SECTION

- Setting Thresholds | 803
- RMON Command-Line Interface | 804
- RMON Event Table | 804
- RMON Alarm Table | 805
- Troubleshooting RMON | 806

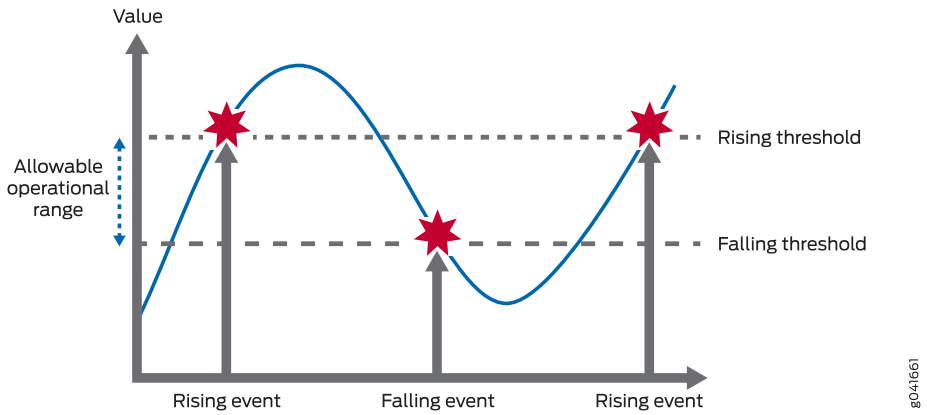
Health and performance monitoring can benefit from the remote monitoring of SNMP variables by the local SNMP agents running on each router. The SNMP agents compare MIB values against predefined thresholds and generate exception alarms without the need for polling by a central SNMP management platform. This is an effective mechanism for proactive management, as long as the thresholds have baselines determined and set correctly. For more information, see RFC 2819, *Remote Network Monitoring MIB*.

This topic includes the following sections:

Setting Thresholds

By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside of the allowable operational range. (See Figure 29 on page 803.)

Figure 29: Setting Thresholds



Events are only generated when the threshold is first crossed in any one direction rather than after each sample period. For example, if a rising threshold crossing event is raised, no more threshold crossing events will occur until a corresponding falling event. This considerably reduces the quantity of alarms that are produced by the system, making it easier for operations staff to react when alarms do occur.

To configure remote monitoring, specify the following pieces of information:

- The variable to be monitored (by its SNMP object identifier)
- The length of time between each inspection
- A rising threshold
- A falling threshold
- A rising event
- A falling event

Before you can successfully configure remote monitoring, you should identify what variables need to be monitored and their allowable operational range. This requires some period of baselining to determine the allowable operational ranges. An initial baseline period of at least three months is not unusual when first identifying the operational ranges and defining thresholds, but baseline monitoring should continue over the life span of each monitored variable.

RMON Command-Line Interface

Junos OS provides two mechanisms you use to control the Remote Monitoring agent on the router: command-line interface (CLI) and SNMP. To configure an RMON entry using the CLI, include the following statements at the **[edit snmp]** hierarchy level:

```
rmon {
    alarm index {
        description;
        falling-event-index;
        falling-threshold;
        intervals;
        rising-event-index;
        rising-threshold;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling | rising | rising-or-falling);
        variable;
    }
    event index {
        community;
        description;
        type (log | trap | log-and-trap | none);
    }
}
```

If you do not have CLI access, you can configure remote monitoring using the SNMP Manager or management application, assuming SNMP access has been granted. (See Table 65 on page 804.) To configure RMON using SNMP, perform SNMP **Set** requests to the RMON event and alarm tables.

RMON Event Table

Set up an event for each type that you want to generate. For example, you could have two generic events, *rising* and *falling*, or many different events for each variable that is being monitored (for example, *temperature rising* event, *temperature falling* event, *firewall hit* event, *interface utilization* event, and so on). Once the events have been configured, you do not need to update them.

Table 65: RMON Event Table

Field	Description
eventDescription	Text description of this event
eventType	Type of event (for example, **log**, **trap**, or **log** and **trap**)

Table 65: RMON Event Table *(continued)*

Field	Description
eventCommunity	Trap group to which to send this event (as defined in the Junos OS configuration, which is not the same as the community)
eventOwner	Entity (for example, **manager**) that created this event
eventStatus	Status of this row (for example, **valid**, **invalid**, or **createRequest**)

RMON Alarm Table

The RMON alarm table stores the SNMP object identifiers (including their instances) of the variables that are being monitored, together with any rising and falling thresholds and their corresponding event indexes. To create an RMON request, specify the fields shown in Table 66 on page 805.

Table 66: RMON Alarm Table

Field	Description
alarmStatus	Status of this row (for example, **valid**, **invalid**, or **createRequest**)
alarmInterval	Sampling period (in seconds) of the monitored variable
alarmVariable	OID (and instance) of the variable to be monitored
alarmValue	Actual value of the sampled variable
alarmSampleType	Sample type (**absolute** or **delta** changes)
alarmStartupAlarm	Initial alarm (**rising**, **falling**, or **either**)
alarmRisingThreshold	Rising threshold against which to compare the value
alarmFallingThreshold	Falling threshold against which to compare the value
alarmRisingEventIndex	Index (row) of the rising event in the event table
alarmFallingEventIndex	Index (row) of the falling event in the event table

Both the **alarmStatus** and **eventStatus** fields are **entryStatus** primitives, as defined in RFC 2579, *Textual Conventions for SMIv2*.

Troubleshooting RMON

You troubleshoot the RMON agent, **rmopd**, that runs on the router by inspecting the contents of the Juniper Networks enterprise RMON MIB, **jnxRmon**, which provides the extensions listed in Table 67 on page 806 to the RFC 2819 **alarmTable**.

Table 67: jnxRmon Alarm Extensions

Field	Description
jnxRmonAlarmGetFailCnt	Number of times the internal **Get** request for the variable failed
jnxRmonAlarmGetFailTime	Value of **sysUpTime** when the last failure occurred
jnxRmonAlarmGetFailReason	Reason why the **Get** request failed
jnxRmonAlarmGetOkTime	Value of **sysUpTime** when the variable moved out of failure state
jnxRmonAlarmState	Status of this alarm entry

Monitoring the extensions in this table provides clues as to why remote alarms may not behave as expected.

RELATED DOCUMENTATION

Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806

Understanding Measurement Points, Key Performance Indicators, and Baseline Values

IN THIS SECTION

- Measurement Points | 807
- Basic Key Performance Indicators | 808
- Setting Baselines | 808

This chapter topic provides guidelines for monitoring the service quality of an IP network. It describes how service providers and network administrators can use information provided by Juniper Networks routers to monitor network performance and capacity. You should have a thorough understanding of the SNMP and the associated MIB supported by Junos OS.

> **NOTE:** For a good introduction to the process of monitoring an IP network, see RFC 2330, *Framework for IP Performance Metrics*.

This topic contains the following sections:

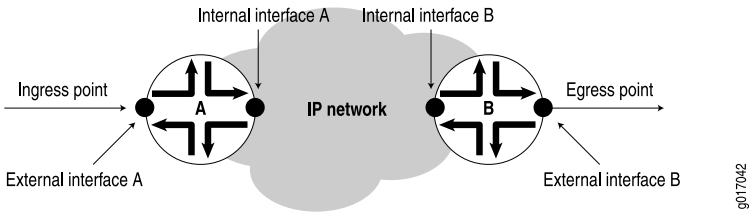
Measurement Points

Defining the measurement points where metrics are measured is equally as important as defining the metrics themselves. This section describes measurement points within the context of this chapter and helps identify where measurements can be taken from a service provider network. It is important to understand exactly where a measurement point is. Measurement points are vital to understanding the implication of what the actual measurement means.

An IP network consists of a collection of routers connected by physical links that are all running the Internet Protocol. You can view the network as a collection of routers with an ingress (entry) point and an egress (exit) point. See Figure 30 on page 807.

- Network-centric measurements are taken at measurement points that most closely map to the ingress and egress points for the network itself. For example, to measure delay across the provider network from Site A to Site B, the measurement points should be the ingress point to the provider network at Site A and the egress point at Site B.
- Router-centric measurements are taken directly from the routers themselves, but be careful to ensure that the correct router subcomponents have been identified in advance.

Figure 30: Network Entry Points



NOTE: Figure 30 on page 807 does not show the client networks at customer premises, but they would be located on either side of the ingress and egress points. Although this chapter does not discuss how to measure network services as perceived by these client networks, you can use measurements taken for the service provider network as input into such calculations.

Basic Key Performance Indicators

For example, you could monitor a service provider network for three basic key performance indicators (KPIs):

- *Availability* measures the "reachability" of one measurement point from another measurement point at the network layer (for example, using ICMP ping). The underlying routing and transport infrastructure of the provider network will support the availability measurements, with failures highlighted as unavailability.
- *Health* measures the number and type of errors that are occurring on the provider network, and can consist of both router-centric and network-centric measurements, such as hardware failures or packet loss.
- *Performance* of the provider network measures how well it can support IP services (for example, in terms of delay or utilization).

Setting Baselines

How well is the provider network performing? We recommend an initial three-month period of monitoring to identify a network's normal operational parameters. With this information, you can recognize exceptions and identify abnormal behavior. You should continue baseline monitoring for the lifetime of each measured metric. Over time, you must be able to recognize performance trends and growth patterns.

Within the context of this chapter, many of the metrics identified do not have an allowable operational range associated with them. In most cases, you cannot identify the allowable operational range until you have determined a baseline for the actual variable on a specific network.

RELATED DOCUMENTATION

Understanding RMON for Monitoring Service Quality | 802

Defining and Measuring Network Availability | 809

Measuring Health | 815

Measuring Performance | 822

Defining and Measuring Network Availability

IN THIS SECTION

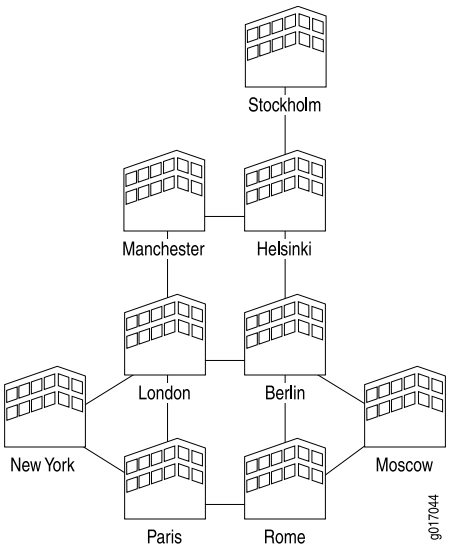
- Defining Network Availability | 809
- Measuring Availability | 811

This topic includes the following sections:

Defining Network Availability

Availability of a service provider's IP network can be thought of as the reachability between the regional points of presence (POP), as shown in Figure 31 on page 809.

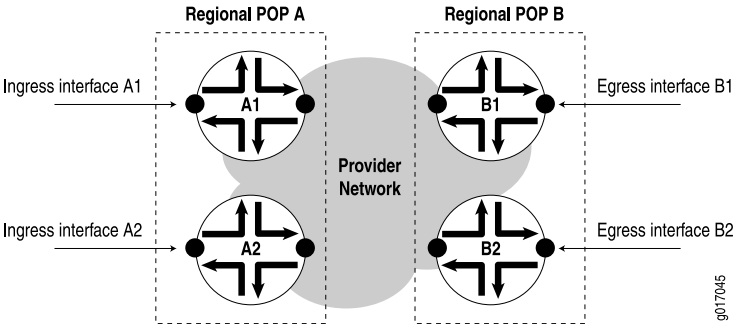
Figure 31: Regional Points of Presence



With the example above, when you use a full mesh of measurement points, where every POP measures the availability to every other POP, you can calculate the total availability of the service provider's network. This KPI can also be used to help monitor the service level of the network, and can be used by the service provider and its customers to determine if they are operating within the terms of their service-level agreement (SLA).

Where a POP may consist of multiple routers, take measurements to each router as shown in Figure 32 on page 810.

Figure 32: Measurements to Each Router



Measurements include:

- Path availability—Availability of an egress interface B1 as seen from an ingress interface A1.
- Router availability—Percentage of path availability of all measured paths terminating on the router.
- POP availability—Percentage of router availability between any two regional POPs, A and B.
- Network availability—Percentage of POP availability for all regional POPs in the service provider's network.

To measure POP availability of POP A to POP B in Figure 32 on page 810, you must measure the following four paths:

```
Path A1 => B1
Path A1 => B2
Path A2 => B1
Path A2 => B2
```

Measuring availability from POP B to POP A would require a further four measurements, and so on.

A full mesh of availability measurements can generate significant management traffic. From the sample diagram above:

- Each POP has two co-located provider edge (PE) routers, each with 2xSTM1 interfaces, for a total of 18 PE routers and 36xSTM1 interfaces.
- There are six core provider (P) routers, four with 2xSTM4 and 3xSTM1 interfaces each, and two with 3xSTM4 and 3xSTM1 interfaces each.

This makes a total of 68 interfaces. A full mesh of paths between every interface is:

[n x (**n**–**l**)] / **2** gives [**68** x (**68**–**1**)] / **2**=**2278** paths

To reduce management traffic on the service provider's network, instead of generating a full mesh of interface availability tests (for example, from each interface to every other interface), you can measure

from each router's loopback address. This reduces the number of availability measurements required to a total of one for each router, or:

[**n** x (**n**–**1**)] / **2** gives [**24** x (**24**–**1**)] / **2**=**276** measurements

This measures availability from each router to every other router.

Monitoring the SLA and the Required Bandwidth

A typical SLA between a service provider and a customer might state:

> A Point of Presence is the connection of two back-to-back provider edge routers to separate core provider routers using different links for resilience. The system is considered to be unavailable when either an entire POP becomes unavailable or for the duration of a Priority 1 fault.

An SLA availability figure of 99.999 percent for a provider's network would relate to a down time of approximately 5 minutes per year. Therefore, to measure this proactively, you would have to take availability measurements at a granularity of less than one every five minutes. With a standard size of 64 bytes per ICMP ping request, one ping test per minute would generate 7680 bytes of traffic per hour per destination, including ping responses. A full mesh of ping tests to 276 destinations would generate 2,119,680 bytes per hour, which represents the following:

- On an OC3/STM1 link of 155.52 Mbps, a utilization of 1.362 percent
- On an OC12/STM4 link of 622.08 Mbps, a utilization of 0.340 percent

With a size of 1500 bytes per ICMP ping request, one ping test per minute would generate 180,000 bytes per hour per destination, including ping responses. A full mesh of ping tests to 276 destinations would generate 49,680,000 bytes per hour, which represents the following:

- On an OC3/STM1 link, 31.94 percent utilization
- On an OC12/STM4 link, 7.986 percent utilization

Each router can record the results for every destination tested. With one test per minute to each destination, a total of 1 x 60 x 24 x 276 = 397,440 tests per day would be performed and recorded by each router. All ping results are stored in the **pingProbeHistoryTable** (see RFC 2925) and can be retrieved by an SNMP performance reporting application (for example, service performance management software from InfoVista, Inc., or Concord Communications, Inc.) for post processing. This table has a maximum size of 4,294,967,295 rows, which is more than adequate.

Measuring Availability

There are two methods you can use to measure availability:

- Proactive—Availability is automatically measured as often as possible by an operational support system.

- Reactive—Availability is recorded by a Help desk when a fault is first reported by a user or a fault monitoring system.

This section discusses real-time performance monitoring as a proactive monitoring solution.

Real-Time Performance Monitoring

Juniper Networks provides a real-time performance monitoring (RPM) service to monitor real-time network performance. Use the J-Web Quick Configuration feature to configure real-time performance monitoring parameters used in real-time performance monitoring tests. (J-Web Quick Configuration is a browser-based GUI that runs on Juniper Networks routers. For more information, see the *J-Web Interface User Guide*.)

Configuring Real-Time Performance Monitoring

Some of the most common options you can configure for real-time performance monitoring tests are shown in Table 68 on page 812.

Table 68: Real-Time Performance Monitoring Configuration Options

Field	Description
Request Information	
Probe Type	Type of probe to send as part of the test. Probe types can be: • **http-get** • **http-get-metadata** • **icmp-ping** • **icmp-ping-timestamp** • **tcp-ping** • **udp-ping**
Interval	Wait time (in seconds) between each probe transmission. The range is 1 to 255 seconds.
Test Interval	Wait time (in seconds) between tests. The range is 0 to 86400 seconds.
Probe Count	Total number of probes sent for each test. The range is 1 to 15 probes.
Destination Port	TCP or UDP port to which probes are sent. Use number 7—a standard TCP or UDP port number—or select a port number from 49152 through 65535.
DSCP Bits	Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is 000000.

Table 68: Real-Time Performance Monitoring Configuration Options *(continued)*

Field	Description
Data Size	Size (in bytes) of the data portion of the ICMP probes. The range is 0 to 65507 bytes.
Data Fill	Contents of the data portion of the ICMP probes. Contents must be a hexadecimal value. The range is 1 to 800h.
Maximum Probe Thresholds	
Successive Lost Probes	Total number of probes that must be lost successively to trigger a probe failure and generate a system log message. The range is 0 to 15 probes.
Lost Probes	Total number of probes that must be lost to trigger a probe failure and generate a system log message. The range is 0 to 15 probes.
Round Trip Time	Total round-trip time (in microseconds) from the Services Router to the remote server, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Jitter	Total jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Standard Deviation	Maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Egress Time	Total one-way time (in microseconds) from the router to the remote server, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Ingress Time	Total one-way time (in microseconds) from the remote server to the router, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.

Table 68: Real-Time Performance Monitoring Configuration Options *(continued)*

Field	Description
Jitter Egress Time	Total outbound-time jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Jitter Ingress Time	Total inbound-time jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Egress Standard Deviation	Maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Ingress Standard Deviation	Maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.

Displaying Real-Time Performance Monitoring Information

For each real-time performance monitoring test configured on the router, monitoring information includes the round-trip time, jitter, and standard deviation. To view this information, select **Monitor > RPM** in the J-Web interface, or enter the **show services rpm** command-line interface (CLI) command.

To display the results of the most recent real-time performance monitoring probes, enter the **show services rpm probe-results** CLI command:

```
user@host> show services rpm probe-results
```

```
Owner: p1, Test: t1
   Target address: 10.8.4.1, Source address: 10.8.4.2, Probe type: icmp-ping
   Destination interface name: lt-0/0/0.0
   Test size: 10 probes
   Probe results:
      Response received, Sun Jul 10 19:07:34 2005
      Rtt: 50302 usec
   Results over current test:
      Probes sent: 2, Probes received: 1, Loss percentage: 50
      Measurement: Round trip time
```

```
      Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
      Jitter: 0 usec, Stddev: 0 usec
Results over all tests:
   Probes sent: 2, Probes received: 1, Loss percentage: 50
   Measurement: Round trip time
     Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
     Jitter: 0 usec, Stddev: 0 usec
```

RELATED DOCUMENTATION

- Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806
- Understanding RMON for Monitoring Service Quality | 802
- Measuring Health | 815
- Measuring Performance | 822

Measuring Health

You can monitor health metrics reactively by using fault management software such as SMARTS InCharge, Micromuse Netcool Omnibus, or Concord Live Exceptions. We recommend that you monitor the health metrics shown in Table 69 on page 815.

Table 69: Health Metrics

Metric	Description	Parameters	
		Name	Value
Errors in	Number of inbound packets that contained errors, preventing them from being delivered	**MIB name**	IF-MIB (RFC 2233)
		Variable name	ifInErrors
		Variable OID	.1.3.6.1.31.2.2.1.14
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	Logical interfaces

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
Errors out	Number of outbound packets that contained errors, preventing them from being transmitted	**MIB name**	IF-MIB (RFC 2233)
		Variable name	ifOutErrors
		Variable OID	.1.3.6.1.31.2.2.1.20
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	Logical interfaces
Discards in	Number of inbound packets discarded, even though no errors were detected	**MIB name**	IF-MIB (RFC 2233)
		Variable name	ifInDiscards
		Variable OID	.1.3.6.1.31.2.2.1.13
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	Logical interfaces
Unknown protocols	Number of inbound packets discarded because they were of an unknown protocol	**MIB name**	IF-MIB (RFC 2233)
		Variable name	ifInUnknownProtos
		Variable OID	.1.3.6.1.31.2.2.1.15
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	Logical interfaces

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
Interface operating status	Operational status of an interface	**MIB name**	IF-MIB (RFC 2233)
		Variable name	ifOperStatus
		Variable OID	.1.3.6.1.31.2.2.1.8
		Frequency (mins)	15
		Allowable range	1 (up)
		Managed objects	Logical interfaces
Label Switched Path (LSP) state	Operational state of an MPLS label-switched path	**MIB name**	MPLS-MIB
		Variable name	mplsLspState
		Variable OID	mplsLspEntry.2
		Frequency (mins)	60
		Allowable range	2 (up)
		Managed objects	All label-switched paths in the network
Component operating status	Operational status of a router hardware component	**MIB name**	JUNIPER-MIB
		Variable name	jnxOperatingState
		Variable OID	.1.3.6.1.4.1.2636.1.13.1.6
		Frequency (mins)	60
		Allowable range	2 (running) or 3 (ready)
		Managed objects	All components in each Juniper Networks router

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
Component operating temperature	Operational temperature of a hardware component, in Celsius	**MIB name**	JUNIPER-MIB
		Variable name	jnxOperatingTemp
		Variable OID	.1.3.6.1.4.1.2636.1.13.1.7
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	All components in a chassis
System up time	Time, in milliseconds, that the system has been operational.	**MIB name**	MIB-2 (RFC 1213)
		Variable name	sysUpTime
		Variable OID	.1.3.6.1.1.3
		Frequency (mins)	60
		Allowable range	Increasing only (decrement indicates a restart)
		Managed objects	All routers
No IP route errors	Number of packets that could not be delivered because there was no IP route to their destination.	**MIB name**	MIB-2 (RFC 1213)
		Variable name	ipOutNoRoutes
		Variable OID	ip.12
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	Each router

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
Wrong SNMP community names	Number of incorrect SNMP community names received	**MIB name**	MIB-2 (RFC 1213)
		Variable name	snmpInBadCommunityNames
		Variable OID	snmp.4
		Frequency (mins)	24
		Allowable range	To be baselined
		Managed objects	Each router
SNMP community violations	Number of valid SNMP communities used to attempt invalid operations (for example, attempting to perform SNMP Set requests)	**MIB name**	MIB-2 (RFC 1213)
		Variable name	snmpInBadCommunityUses
		Variable OID	snmp.5
		Frequency (mins)	24
		Allowable range	To be baselined
		Managed objects	Each router
Redundancy switchover	Total number of redundancy switchovers reported by this entity	**MIB name**	JUNIPER-MIB
		Variable name	jnxRedundancySwitchoverCount
		Variable OID	jnxRedundancyEntry.8
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	All Juniper Networks routers with redundant Routing Engines

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
FRU state	Operational status of each field-replaceable unit (FRU)	**MIB name**	JUNIPER-MIB
		Variable name	jnxFruState
		Variable OID	jnxFruEntry.8
		Frequency (mins)	15
		Allowable range	2 through 6 for ready/online states. See jnxFruOfflineReason in the event of a FRU failure.
		Managed objects	All FRUs in all Juniper Networks routers.
Rate of tail-dropped packets	Rate of tail-dropped packets per output queue, per forwarding class, per interface.	**MIB name**	JUNIPER-COS-MIB
		Variable name	jnxCosIfqTailDropPktRate
		Variable OID	jnxCosIfqStatsEntry.12
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	For each forwarding class per interface in the provider network, when CoS is enabled.

Table 69: Health Metrics *(continued)*

Metric	Description	Parameters	
		Name	Value
Interface utilization: octets received	Total number of octets received on the interface, including framing characters.	**MIB name**	IF-MIB
		Variable name	ifInOctets
		Variable OID	.1.3.6.1.2.1.2.2.1.10.x
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	All operational interfaces in the network
Interface utilization: octets transmitted	Total number of octets transmitted out of the interface, including framing characters.	**MIB name**	IF-MIB
		Variable name	ifOutOctets
		Variable OID	.1.3.6.1.2.1.2.2.1.16.x
		Frequency (mins)	60
		Allowable range	To be baselined
		Managed objects	All operational interfaces in the network

NOTE: Byte counts vary depending on interface type, encapsulation used and PIC supported. For example, with vlan-ccc encapsulation on a 4xFE, GE, or GE 1Q PIC, the byte count includes framing and control word overhead. (See Table 70 on page 822.)

Table 70: Counter Values for vlan-ccc Encapsulation

PIC Type	Encapsulation	input (Unit Level)	Output (Unit Level)	SNMP
4xFE	vlan-ccc	Frame (no frame check sequence [FCS])	Frame (including FCS and control word)	ifInOctets, ifOutOctets
GE	vlan-ccc	Frame (no FCS)	Frame (including FCS and control word)	ifInOctets, ifOutOctets
GE IQ	vlan-ccc	Frame (no FCS)	Frame (including FCS and control word)	ifInOctets, ifOutOctets

SNMP traps are also a good mechanism to use for health management. For more information, see ""Standard SNMP Traps Supported by Junos OS" on page 490" and ""Enterprise-Specific SNMP Traps Supported by Junos OS" on page 500."

RELATED DOCUMENTATION

- Understanding Measurement Points, Key Performance Indicators, and Baseline Values | 806
- Understanding RMON for Monitoring Service Quality | 802
- Defining and Measuring Network Availability | 809
- Measuring Performance | 822
- SNMB MIB Explorer

Measuring Performance

IN THIS SECTION

- Measuring Class of Service | 825
- Inbound Firewall Filter Counters per Class | 826
- Monitoring Output Bytes per Queue | 828
- Dropped Traffic | 829

The performance of a service provider's network is usually defined as how well it can support services, and is measured with metrics such as delay and utilization. We suggest that you monitor the following performance metrics using applications such as InfoVista Service Performance Management or Concord Network Health (see Table 71 on page 823).

Table 71: Performance Metrics

Metric:	Average delay
Description	Average round-trip time (in milliseconds) between two measurement points.
MIB name	DISMAN-PING-MIB (RFC 2925)
Variable name	**pingResultsAverageRtt**
Variable OID	pingResultsEntry.6
Frequency (mins)	15 (or depending upon ping test frequency)
Allowable range	To be baselined
Managed objects	Each measured path in the network
Metric:	Interface utilization
Description	Utilization percentage of a logical connection.
MIB name	IF-MIB
Variable name	(**ifInOctets** & **ifOutOctets**) * 8 / **ifSpeed**
Variable OID	ifTable entries
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All operational interfaces in the network
Metric:	Disk utilization
Description	Utilization of disk space within the Juniper Networks router
MIB name	HOST-RESOURCES-MIB (RFC 2790)

Table 71: Performance Metrics *(continued)*

Variable name	**hrStorageSize** – **hrStorageUsed**
Variable OID	hrStorageEntry.5 – hrStorageEntry.6
Frequency (mins)	1440
Allowable range	To be baselined
Managed objects	All Routing Engine hard disks
Metric:	Memory utilization
Description	Utilization of memory on the Routing Engine and FPC.
MIB name	JUNIPER-MIB (Juniper Networks enterprise Chassis MIB)
Variable name	**jnxOperatingHeap**
Variable OID	Table for each component
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All Juniper Networks routers
Metric:	CPU load
Description	Average utilization over the past minute of a CPU.
MIB name	JUNIPER-MIB (Juniper Networks enterprise Chassis MIB)
Variable name	**jnxOperatingCPU**
Variable OID	Table for each component
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All Juniper Networks routers
Metric:	LSP utilization

Table 71: Performance Metrics *(continued)*

Description	Utilization of the MPLS label-switched path.
MIB name	MPLS-MIB
Variable name	**mplsPathBandwidth / (mplsLspOctets * 8)**
Variable OID	mplsLspEntry.21 and mplsLspEntry.3
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All label-switched paths in the network
Metric:	Output queue size
Description	Size, in packets, of each output queue per forwarding class, per interface.
MIB name	JUNIPER-COS-MIB
Variable name	**jnxCosIfqQedPkts**
Variable OID	jnxCosIfqStatsEntry.3
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	For each forwarding class per interface in the network, once CoS is enabled.

This section includes the following topics:

Measuring Class of Service

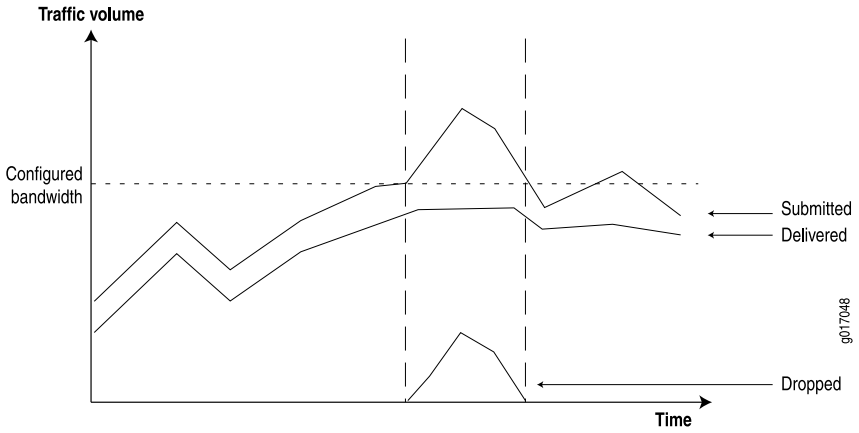
You can use class-of-service (CoS) mechanisms to regulate how certain classes of packets are handled within your network during times of peak congestion. Typically you must perform the following steps when implementing a CoS mechanism:

- Identify the type of packets that is applied to this class. For example, include all customer traffic from a specific ingress edge interface within one class, or include all packets of a particular protocol such as voice over IP (VoIP).

- Identify the required deterministic behavior for each class. For example, if VoIP is important, give VoIP traffic the highest priority during times of network congestion. Conversely, you can downgrade the importance of Web traffic during congestion, as it may not impact customers too much.

With this information, you can configure mechanisms at the network ingress to monitor, mark, and police traffic classes. Marked traffic can then be handled in a more deterministic way at egress interfaces, typically by applying different queuing mechanisms for each class during times of network congestion. You can collect information from the network to provide customers with reports showing how the network is behaving during times of congestion. (See Figure 33 on page 826.)

Figure 33: Network Behavior During Congestion



To generate these reports, routers must provide the following information:

- Submitted traffic—Amount of traffic received per class.
- Delivered traffic—Amount of traffic transmitted per class.
- Dropped traffic—Amount of traffic dropped because of CoS limits.

The following section outlines how this information is provided by Juniper Networks routers.

Inbound Firewall Filter Counters per Class

Firewall filter counters are a very flexible mechanism you can use to match and count inbound traffic per class, per interface. For example:

```
firewall {
   filter f1 {
      term t1 {
         from {
            dscp af11;
         }
```

```
            then {
                # Assured forwarding class 1 drop profile 1 count inbound-af11;
                accept;
            }
        }
    }
}
```

For example, Table 72 on page 827 shows additional filters used to match the other classes.

Table 72: Inbound Traffic Per Class

DSCP Value	Firewall Match Condition	Description
10	af11	Assured forwarding class 1 drop profile 1
12	af12	Assured forwarding class 1 drop profile 2
18	af21	Best effort class 2 drop profile 1
20	af22	Best effort class 2 drop profile 2
26	af31	Best effort class 3 drop profile 1

Any packet with a CoS DiffServ code point (DSCP) conforming to RFC 2474 can be counted in this way. The Juniper Networks enterprise-specific Firewall Filter MIB presents the counter information in the variables shown in Table 73 on page 827.

Table 73: Inbound Counters

Indicator Name	Inbound Counters
MIB	**jnxFirewalls**
Table	**jnxFirewallCounterTable**
Index	**jnxFWFilter.jnxFWCounter**
Variables	**jnxFWCounterPacketCount** **jnxFWCounterByteCount**
Description	Number of bytes being counted pertaining to the specified firewall filter counter

Table 73: Inbound Counters *(continued)*

Indicator Name	Inbound Counters
SNMP version	SNMPv2

This information can be collected by any SNMP management application that supports SNMPv2. Products from vendors such as Concord Communications, Inc., and InfoVista, Inc., provide support for the Juniper Networks Firewall MIB with their native Juniper Networks device drivers.

Monitoring Output Bytes per Queue

You can use the Juniper Networks enterprise ATM CoS MIB to monitor outbound traffic, per virtual circuit forwarding class, per interface. (See Table 74 on page 828.)

Table 74: Outbound Counters for ATM Interfaces

Indicator Name	Outbound Counters
MIB	**JUNIPER-ATM-COS-MIB**
Variable	**jnxCosAtmVcQstatsOutBytes**
Index	**ifIndex.atmVclVpi.atmVclVci.jnxCosFcId**
Description	Number of bytes belonging to the specified forwarding class that were transmitted on the specified virtual circuit.
SNMP version	SNMPv2

Non-ATM interface counters are provided by the Juniper Networks enterprise-specific CoS MIB, which provides information shown in Table 75 on page 828.

Table 75: Outbound Counters for Non-ATM Interfaces

Indicator Name	Outbound Counters
MIB	**JUNIPER-COS-MIB**
Table	**jnxCosIfqStatsTable**
Index	**jnxCosIfqIfIndex.jnxCosIfqFc**
Variables	**jnxCosIfqTxedBytes** **jnxCosIfqTxedPkts**

Table 75: Outbound Counters for Non-ATM Interfaces *(continued)*

Indicator Name	Outbound Counters
Description	Number of transmitted bytes or packets per interface per forwarding class
SNMP version	SNMPv2

Dropped Traffic

You can calculate the amount of dropped traffic by subtracting the outbound traffic from the incoming traffic:

```
Dropped = Inbound Counter – Outbound Counter
```

You can also select counters from the CoS MIB, as shown in Table 76 on page 829.

Table 76: Dropped Traffic Counters

Indicator Name	Dropped Traffic
MIB	**JUNIPER-COS-MIB**
Table	**jnxCosIfqStatsTable**
Index	**jnxCosIfqIfIndex.jnxCosIfqFc**
Variables	**jnxCosIfqTailDropPkts** **jnxCosIfqTotalRedDropPkts**
Description	The number of tail-dropped or RED-dropped packets per interface per forwarding class
SNMP version	SNMPv2

RELATED DOCUMENTATION

- Understanding Measurement Points, Key Performance Indicators, and Baseline Values | **806**
- Understanding RMON for Monitoring Service Quality | **802**
- Defining and Measuring Network Availability | **809**

CHAPTER 21

Health Monitoring with SNMP

IN THIS CHAPTER

- Understanding Health Monitoring | 831
- Configuring Health Monitoring | 832
- Configuring Health Monitoring on Devices Running Junos OS | 834
- Example: Configuring Health Monitoring | 837

Understanding Health Monitoring

Health monitoring is an SNMP feature that extends the RMON alarm infrastructure to provide monitoring for a predefined set of objects (such as file system usage, CPU usage, and memory usage), and for Junos OS processes.

You enable the health monitor feature using the **health-monitor** statement at the **[edit snmp]** hierarchy level. You can also configure health monitor parameters such as a falling threshold, rising threshold, and interval. If the value of a monitored object exceeds the rising or falling threshold, an alarm is triggered and an event may be logged.

The falling threshold is the lower threshold for the monitored object instance. The rising threshold is the upper threshold for the monitored object instance. Each threshold is expressed as a percentage of the maximum possible value. The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

Events are only generated when a threshold is first crossed in any one direction, rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs.

System log entries for health monitor events have a corresponding HEALTHMONITOR tag and not a generic SNMPD_RMON_EVENTLOG tag. However, the health monitor sends generic RMON risingThreshold and fallingThreshold traps. You can use the **show snmp health-monitor** operational command to view information about health monitor alarms and logs.

When you configure the health monitor, monitoring information for certain object instances is available, as shown in Table 77 on page 832.

Table 77: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed.1	Monitors the **/dev/ad0s1a:** file system on the switch. This is the root file system mounted on /.
jnxHrStoragePercentUsed.2	Monitors the **/dev/ad0s1e:** file system on the switch. This is the configuration file system mounted on **/config**.
jnxOperatingCPU (RE0)	Monitors CPU usage by the Routing Engine (RE0).
jnxOperatingBuffer (RE0)	Monitors the amount of memory available on the Routing Engine (RE0).
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS process. Multiple instances of the same process are monitored and indexed separately.

RELATED DOCUMENTATION

Configuring Health Monitoring | **832**

falling-threshold (Health Monitor) | **2166**

interval (Health Monitor) | **2180**

rising-threshold (Health Monitor) | **2214**

show snmp health-monitor

Configuring Health Monitoring

This topic describes how to configure the health monitor feature for QFX Series and OCX Series devices.

The health monitor feature extends the SNMP RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (such as file system usage, CPU usage, and memory usage) and dynamic object instances (such as Junos OS processes).

To configure health monitoring:

1. Configure the health monitor:

```
[edit snmp]
user@switch# set health-monitor
```

2. Configure the falling threshold:

```
[edit snmp]
user@switch# set health-monitor falling-threshold percentage
```

For example:

```
user@switch# set health-monitor falling-threshold 85
```

3. Configure the rising threshold:

```
[edit snmp]
user@switch# set health-monitor rising-threshold percentage
```

For example:

```
user@switch# set health-monitor rising-threshold 75
```

4. Configure the interval:

```
[edit snmp]
user@switch# set health-monitor interval seconds
```

For example:

```
user@switch# set health-monitor interval 600
```

RELATED DOCUMENTATION

Understanding Health Monitoring | 831

falling-threshold | 2166

interval (Health Monitor) | 2180

rising-threshold (Health Monitor) | 2214

Configuring Health Monitoring on Devices Running Junos OS

IN THIS SECTION

- Monitored Objects | 835
- Minimum Health Monitoring Configuration | 836
- Configuring the Falling Threshold or Rising Threshold | 836
- Configuring the Interval | 837
- Log Entries and Traps | 837

As the number of devices managed by a typical network management system (NMS) grows and the complexity of the devices themselves increases, it becomes increasingly impractical for the NMS to use polling to monitor the devices. A more scalable approach is to rely on network devices to notify the NMS when something requires attention.

On Juniper Networks routers, RMON alarms and events provide much of the infrastructure needed to reduce the polling overhead from the NMS. However, with this approach, you must set up the NMS to configure specific MIB objects into RMON alarms. This often requires device-specific expertise and customizing of the monitoring application. In addition, some MIB object instances that need monitoring are set only at initialization or change at runtime and cannot be configured in advance.

To address these issues, the health monitor extends the RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (for file system usage, CPU usage, and memory usage) and includes support for unknown or dynamic object instances (such as Junos OS processes).

Health monitoring is designed to minimize user configuration requirements. To configure health monitoring entries, include the **health-monitor** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
health-monitor {
   falling-threshold percentage;
   interval seconds;
   rising-threshold percentage;
   idp {
      falling-threshold percentage;
      interval seconds;
      rising-threshold percentage;
   }
}
```

Configuring monitoring events at the **[edit snmp health-monitor]** hierarchy level sets polling intervals for the overall system health. If you set these same options at the **[edit snmp health-monitor idp]** hierarchy level, an SNMP event is generated by the device if the percentage of dataplane memory utilized by the intrusion detection and prevention (IDP) system rises above or falls below your settings.

You can use the **show snmp health-monitor** operational command to view information about health monitor alarms and logs.

This topic describes the minimum required configuration and discusses the following tasks for configuring the health monitor:

Monitored Objects

When you configure the health monitor, monitoring information for certain object instances is available, as shown in Table 78 on page 835.

Table 78: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed1	Monitors the following file system on the router or switch: **/dev/ad0s1a:** This is the root file system mounted on /.
jnxHrStoragePercentUsed2	Monitors the following file system on the router or switch: **/dev/ad0s1e:** This is the configuration file system mounted on **/config**.
jnxOperatingCPU (RE0) **jnxOperatingCPU (RE1)**	Monitors CPU usage for Routing Engines (**RE0** and **RE1**). The index values assigned to Routing Engines depend on whether the Chassis MIB uses a zero-based or ones-based indexing scheme. Because the indexing scheme is configurable, the proper index is determined when the router or switch is initialized and when there is a configuration change. If the router or switch has only one Routing Engine, the alarm entry monitoring **RE1** is removed after five failed attempts to obtain the CPU value.
jnxOperatingBuffer (RE0) **jnxOperatingBuffer (RE1)**	Monitors the amount of memory available on Routing Engines (**RE0** and **RE1**). Because the indexing of this object is identical to that used for **jnxOperatingCPU**, index values are adjusted depending on the indexing scheme used in the Chassis MIB. As with **jnxOperatingCPU**, the alarm entry monitoring **RE1** is removed if the router or switch has only one Routing Engine.
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.

Table 78: Monitored Object Instances *(continued)*

Object	Description
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS process. Multiple instances of the same process are monitored and indexed separately.

Minimum Health Monitoring Configuration

To enable health monitoring on the router or switch, include the **health-monitor** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
health-monitor;
```

Configuring the Falling Threshold or Rising Threshold

The falling threshold is the lower threshold (expressed as a percentage of the maximum possible value) for the monitored variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising threshold. You must specify the falling threshold as a percentage of the maximum possible value. The default is **70** percent.

By default, the rising threshold is **80** percent of the maximum possible value for the monitored object instance. The rising threshold is the upper threshold for the monitored variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. You must specify the rising threshold as a percentage of the maximum possible value for the monitored variable.

To configure the falling threshold or rising threshold, include the **falling-threshold** or **rising-threshold** statement at the **[edit snmp health-monitor]** hierarchy level:

```
[edit snmp health-monitor]
falling-threshold percentage;
rising-threshold percentage;
```

percentage can be a value from **1** through **100**.

The falling and rising thresholds apply to all object instances monitored by the health monitor.

Configuring the Interval

The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

To configure the interval, include the **interval** statement and specify the number of seconds at the **[edit snmp health-monitor]** hierarchy level:

```
[edit snmp health-monitor]
interval seconds;
```

seconds can be a value from **1** through **2147483647**. The default is **300** seconds (5 minutes).

Log Entries and Traps

The system log entries generated for any health monitor events (thresholds crossed, errors, and so on) have a corresponding **HEALTHMONITOR** tag rather than a generic **SNMPD_RMON_EVENTLOG** tag. However, the health monitor sends generic RMON **risingThreshold** and **fallingThreshold** traps.

RELATED DOCUMENTATION

- Understanding RMON Alarms and Events Configuration | 780
- Configuring an RMON Alarm Entry and Its Attributes | 784
- Configuring an RMON Event Entry and Its Attributes | 789
- Example: Configuring Health Monitoring | 837
- Understanding Device Management Functions in Junos OS | 2
- health-monitor | 2013

Example: Configuring Health Monitoring

Configure the health monitor:

```
[edit snmp]
health-monitor {
    falling-threshold 85;
    interval 600;
```

```
    rising-threshold 75;
}
```

In this example, the sampling interval is every **600** seconds (10 minutes), the falling threshold is **85** percent of the maximum possible value for each object instance monitored, and the rising threshold is **75** percent of the maximum possible value for each object instance monitored.

RELATED DOCUMENTATION

Configuring Health Monitoring on Devices Running Junos OS | **834**

PART 6

Accounting Options, Source Class Usage, and Destination Class Usage Options

Accounting Options, Source Class Usage and Destination Class Usage Options Overview | **840**

Configuring Accounting Options, Source Class Usage and Destination Class Usage Options | **844**

CHAPTER 22

Accounting Options, Source Class Usage and Destination Class Usage Options Overview

IN THIS CHAPTER

- Accounting Options Overview | 840
- Understanding Source Class Usage and Destination Class Usage Options | 841

Accounting Options Overview

An accounting profile represents common characteristics of collected accounting data, including the following:

- Collection interval
- File to contain accounting data
- Specific fields and counter names on which to collect statistics

You can configure multiple accounting profiles, as described in Table 79 on page 840.

Table 79: Types of Accounting Profiles

Type of Profile	Description
Interface profile	Collects the specified error and statistic information.
Filter profile	Collects the byte and packet counts for the counter names specified in the filter profile.
MIB profile	Collects selected MIB statistics and logs them to a specified file.
Routing Engine profile	Collects selected Routing Engine statistics and logs them to a specified file.

Table 79: Types of Accounting Profiles *(continued)*

Type of Profile	Description
Class usage profile	Collects class usage statistics and logs them to a specified file.

RELATED DOCUMENTATION

- Understanding Device Management Functions in Junos OS | 2
- Accounting Options Configuration
- Configuring Accounting-Data Log Files | 856
- Configuring the Interface Profile
- Configuring the Filter Profile | 868
- Configuration Statements at the [edit accounting-options] Hierarchy Level | 844

Understanding Source Class Usage and Destination Class Usage Options

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 lookups on the IP source address and the IP destination 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.

Destination class usage (DCU) counts packets from customers by performing lookups 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.

On T Series Core Routers and M320 Multiservice Edge Routers, the source class and destination classes are not carried across the platform fabric. The implications of this are as follows:

- On T Series and M320 routers, SCU and DCU accounting is performed before the packet enters the fabric.
- On T Series and M320 routers, DCU is performed before output filters are evaluated.
- On M Series platforms, DCU is performed after output filters are evaluated.

- If an output filter drops traffic on M Series devices, the dropped packets are excluded from DCU statistics.
- If an output filter drops traffic on T Series and M320 routers, the dropped packets are included in DCU statistics.

> **NOTE:** For PTX Series routers with FPC3, and PTX1000 routers, to support SCU and DCU, you must configure *enhanced-mode* on the chassis.

On MX Series platforms with MPC/MIC interfaces, SCU and DCU are performed after output filters are evaluated. Packets dropped by output filters are not included in SCU or DCU statistics.

On MX Series platforms with non-MPC/MIC interfaces, SCU and DCU are performed before output filters are evaluated. Packets dropped by output filters are included in SCU and DCU statistics.

On PTX Series platforms, SCU and DCU accounting is performed before output filters are evaluated. Packets dropped by output filters are included in SCU and DCU statistics. On PTX10003, PTX10004, PTX10008, PTX10001-36MR, and line card JNP10K-LC1201, the systems prefixes with SCU and DCU classes assigned occupy more space in the forwarding information base (FIB) tables than regular routes. You must limit the number of prefixes with non-default class assigned.

On Enhanced Scaling FPCs (T640-FPC1-ES, T640-FPC2-ES, T640-FPC3-ES, T640-FPC4-1P-ES , and T1600-FPC4-ES), the source class accounting is performed at ingress. Starting with Junos OS Release 14.2, the SCU accounting is performed at ingress on a T4000 Type 5 FPC. The implications of this are as follows:

- SCU accounting is performed when packets traverse from T4000 Type 5 FPC (ingress FPC) to Enhanced Scaling FPCs (egress FPC).
- SCU accounting is performed when packets traverse from Enhanced Scaling FPCs (ingress FPC) to T4000 Type 5 FPC (egress FPC).

> **NOTE:** When the interface statistics are cleared and then the routing engine is replaced, the SCU and DCU statistics will not match the statistics of the previous routing engine.

For more information about source class usage, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide* and the *Junos OS Network Interfaces Library for Routing Devices*.

RELATED DOCUMENTATION

Example: Grouping Source and Destination Prefixes into a Forwarding Class

Configuring SCU or DCU | **873**

Configuring SCU on a Virtual Loopback Tunnel Interface | 876

Configuring Class Usage Profiles | 878

Configuring the MIB Profile | 881

Configuring the Routing Engine Profile | 884

CHAPTER 23

Configuring Accounting Options, Source Class Usage and Destination Class Usage Options

IN THIS CHAPTER

- Configuration Statements at the [edit accounting-options] Hierarchy Level | 844
- Accounting Options Configuration | 846
- Configuring Accounting-Data Log Files | 856
- Managing Accounting Files | 862
- Configuring the Interface Profile | 864
- Configuring the Filter Profile | 868
- Example: Configuring a Filter Profile | 870
- Example: Configuring Interface-Specific Firewall Counters and Filter Profiles | 871
- Configuring SCU or DCU | 873
- Configuring SCU on a Virtual Loopback Tunnel Interface | 876
- Configuring Class Usage Profiles | 878
- Configuring the MIB Profile | 881
- Configuring the Routing Engine Profile | 884

Configuration Statements at the [edit accounting-options] Hierarchy Level

This topic shows all possible configuration statements at the **[edit accounting-options]** hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

```
[edit]
accounting-options {
   class-usage-profile profile-name {
      file filename;
      interval minutes;
      destination-classes {
```

```
            destination-class-name;
        }
        source-classes {
            source-class-name;
        }
    }
    file filename {
        archive-sites {
        }
        files number;
        nonpersistent;
        size bytes;
        start-time time;
        transfer-interval minutes;
    }
    filter-profile profile-name {
        counters {
            counter-name;
        }
        file filename;
        interval minutes;
    }
}
interface-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
mib-profile profile-name {
    file filename;
    interval seconds;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
```

```
}
```

RELATED DOCUMENTATION

Accounting Options Overview | 840
Accounting Options Configuration | 846

Accounting Options Configuration

IN THIS SECTION

Accounting Options—Full Configuration | 846
Minimum Accounting Options Configuration | 851

This topic contains the following sections:

Accounting Options—Full Configuration

To configure accounting options, include the following statements at the **[edit accounting-options]** hierarchy level:

```
accounting-options {
   class-usage-profile profile-name {
      file filename;
      interval minutes;
      destination-classes {
         destination-class-name;
      }
      source-classes {
         source-class-name;
      }
      file filename {
         archive-sites {
            site-name;
```

```
        }
        files number;
        nonpersistent;
        size bytes;
        source-classes time;
        transfer-interval minutes;
    }
    filter-profile profile-name {
        counters {
            counter-name;
        }
        file filename;
        interval minutes;
    }
}
flat-file-profile profile-name{
    fields {
        all-fields;
        egress-stats {
            all-fields;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
            total-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            vlan-id;
        }
        ingress-stats {
            all-fields;
```

```
        drop-packets;
        input-bytes;
        input-packets;
        output-bytes;
        output-packets;
        queue-id;
    }
    l2-stats {
        all-fields;
        input-mcast-bytes;
        input-mcast-packets;
    }
    fields {
        all-fields;
        egress-stats {
            all-fields;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
            total-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            vlan-id;
        }
        ingress-stats {
            all-fields;
            drop-packets;
            input-bytes;
            input-packets;
            output-bytes;
```

```
    output-packets;
    queue-id;
}
general-param {
    all-fields;
    accounting-type;
    descr;
    line-id;
    logical-interface;
    nas-port-id;
    physical-interface;
    routing-instance;
    timestamp;
    vlan-id;
}
ingress-stats {
    all-fields;
    drop-packets;
    input-bytes;
    input-packets;
    output-bytes;
    output-packets;
    queue-id;
}
l2-stats {
    all-fields;
    input-mcast-bytes;
    input-mcast-packets;
}
overall-packet {
    all-fields;
    input-bytes;
    input-discards;
    input-errors;
    input-packets;
    inputv6-bytes;
    inputv6-packets;
    output-bytes;
    output-errors;
    output-packets;
    outputv6-bytes;
    outputv6-packets;
    input-v4-bytes;
    input-v4-packets;
```

```
                output-v4-bytes;
                output-v4-packets;
                input-bytes-per-sec;
                input-packets-per-sec;
            }
        }
        file filename;
        format (csv | ipdr)
        interval minutes;
        schema-version schema-name;
    }
    interface-profile profile-name {
        fields {
            field-name;
        }
        file filename;
        interval minutes;
    }
    mib-profile profile-name {
        file filename;
        interval (Accounting Options) seconds;
        object-names {
            mib-object-name;
        }
        operation operation-name;
    }
    routing-engine-profile profile-name {
        fields {
            field-name;
        }
        file filename;
        interval minutes;
    }
  }
}
```

By default, accounting options are disabled.

NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because doing so can cause the SNMP walk or a CLI show command to time out.

Minimum Accounting Options Configuration

To enable accounting options on the router, you must perform at least the following tasks:

- Configure accounting options by including a **file** statement and one or more **source-class-usage**, **destination-class-profile**, **filter-profile**, **interface-profile**, **mib-profile**, or **routing-engine-profile** statements at the **[edit accounting-options]** hierarchy level:

```
[edit]
accounting-options {
   class-usage-profile profile-name {
      file filename;
      interval minutes;
      source-classes {
         source-class-name;
      }
      destination-classes {
         destination-class-name;
      }
      file filename {
         archive-sites {
            site-name;
         }
         files number;
         size bytes;
         transfer-interval minutes;
      }
      filter-profile profile-name {
         counters {
            counter-name;
         }
         file filename;
         interval minutes;
      }
      flat-file-profile profile-name{
         fields {
            all-fields;
            egress-stats {
               all-fields;
               input-bytes;
               input-packets;
               output-bytes;
               output-packets;
               queue-id;
               red-drop-bytes;
```

```
        red-drop-packets;
        tail-drop-packets;
        total-drop-packets;
    }
    general-param {
        all-fields;
        accounting-type;
        descr;
        line-id;
        logical-interface;
        nas-port-id;
        physical-interface;
        routing-instance;
        timestamp;
        vlan-id;
    }
    ingress-stats {
        all-fields;
        drop-packets;
        input-bytes;
        input-packets;
        output-bytes;
        output-packets;
        queue-id;
    }
    l2-stats {
        all-fields;
        input-mcast-bytes;
        input-mcast-packets;
    }
    overall-packet {
        all-fields;
        input-bytes;
        input-discards;
        input-errors;
        input-packets;
        inputv6-bytes;
        inputv6-packets;
        output-bytes;
        output-errors;
        output-packets;
        outputv6-bytes;
        outputv6-packets;
        input-v4-bytes;
```

```
            input-v4-packets;
            output-v4-bytes;
            output-v4-packets;
            input-bytes-per-sec;
            input-packets-per-sec;
        }
    }
    file filename;
    format (csv | ipdr)
    interval minutes;
    schema-version schema-name;
}
flat-file-profile profile-name{
    fields {
        all-fields;
        egress-stats {
            all-fields;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
            total-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            vlan-id;
        }
        ingress-stats {
            all-fields;
            drop-packets;
            input-bytes;
            input-packets;
```

```
            output-bytes;
            output-packets;
            queue-id;
        }
        l2-stats {
            all-fields;
            input-mcast-bytes;
            input-mcast-packets;
        }
        overall-packet {
            all-fields;
            input-bytes;
            input-discards;
            input-errors;
            input-packets;
            inputv6-bytes;
            inputv6-packets;
            output-bytes;
            output-errors;
            output-packets;
            outputv6-bytes;
            outputv6-packets;
            input-v4-bytes;
            input-v4-packets;
            output-v4-bytes;
            output-v4-packets;
            input-bytes-per-sec;
            input-packets-per-sec;
        }
    }
    file filename;
    format (csv | ipdr)
    interval minutes;
    schema-version schema-name;
}
interface-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
mib-profile profile-name {
    file filename;
```

```
        interval minutes;
        object-names {
            mib-object-name;
        }
        operation operation-name;
    }
    routing-engine-profile profile-name {
        fields {
            field-name;
        }
        file filename;
        interval minutes;
    }
  }
}
```

- Apply the profiles to the chosen interfaces or filters.

  Apply an interface profile to a physical or logical interface by including the **accounting-profile** statement at either the **[edit interfaces *interface-name*]** or the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

```
[edit interfaces]
interface-name {
    accounting-profile profile-name;
    unit logical-unit-number {
        accounting-profile profile-name;
    }
}
```

> **NOTE:** You do not apply destination class profiles to interfaces. Although the interface needs to have the **destination-class-usage** statement configured, the destination class profile automatically finds all interfaces with the destination class configured.

  Apply a filter profile to a firewall filter by including the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level:

```
[edit firewall]
filter filter-name {
    accounting-profile profile-name;
}
```

You do not need to apply the Routing Engine profile to an interface because the statistics are collected on the Routing Engine itself.

RELATED DOCUMENTATION

- Accounting Options Overview | 840
- Understanding Device Management Functions in Junos OS | 2
- Configuring Accounting-Data Log Files | 856
- Configuring the Interface Profile | 864
- Configuring the Filter Profile | 868
- Configuration Statements at the [edit accounting-options] Hierarchy Level | 844

Configuring Accounting-Data Log Files

IN THIS SECTION

- Configuring How Long Backup Files Are Retained | 857
- Configuring the Maximum Size of the File | 858
- Configuring Archive Sites for the Files | 858
- Configuring Local Backup for Accounting Files | 859
- Configuring Files to Be Compressed | 859
- Configuring the Maximum Number of Files | 860
- Configuring the Storage Location of the File | 860
- Configuring Files to Be Saved After a Change in Mastership | 860
- Configuring the Start Time for File Transfer | 861
- Configuring the Transfer Interval of the File | 861

An accounting profile specifies what statistics to collect and write to a log file. To configure an accounting-data log file, include the **file** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
cleanup-interval {
```

```
    interval days;
}
file filename {
    archive-sites {
        site-name;
    }
    backup-on-failure (master-and-slave | master-only);
    files number;
    nonpersistent;
    push-backup-to-master;
    size bytes;
    start-time time;
    transfer-interval minutes;
}
```

where ***filename*** is the name of the file in which to write accounting data.

If the filename contains spaces, enclose it in quotation marks (" "). The filename cannot contain a forward slash (/). The file is created in the **/var/log** directory and can contain data from multiple profiles.

All accounting-data log files include header and trailer sections that start with a **#** in the first column. The header contains the file creation time, the hostname, and the columns that appear in the file. The trailer contains the time that the file was closed.

Whenever any configured value changes that affects the columns in a file, the file creates a new profile layout record that contains a new list of columns.

You must configure the file size; all other properties are optional.

Configuring How Long Backup Files Are Retained

You can configure how many days the files are retained in the local directory before they are deleted.

> **NOTE:** Files saved to the **/var/log/pfedBackup** directory are always compressed to conserve local storage, regardless of whether the **compress** statement is configured.

To configure retention for backup files:

- Specify the number of days.

```
[edit accounting-options]
user@host# set cleanup-interval interval days
```

> **NOTE:** Files are retained for 1 day if you do not configure this option.

This value, whether configured or default, applies to all configured files at the **[edit accounting-options file]** hierarchy level.

Configuring the Maximum Size of the File

To configure the maximum size of the file:

- Specify the size.

```
[edit accounting-options file filename]
size bytes;
```

The **size** statement is the maximum size of the log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). The minimum value for ***bytes*** is 256 KB. You must configure ***bytes***; the remaining attributes are optional.

Configuring Archive Sites for the Files

After a file reaches its maximum size or the **transfer-interval** time is exceeded, the file is closed, renamed, and, if you configured an archive site, transferred to a remote host.

To configure the sites where files are archived:

- Specify one or more site names.

```
[edit accounting-options file filename]
user@host# set archive-sites site-name
```

where ***site-name*** is any valid FTP URL. For more information about specifying valid FTP URLs, see the *Junos OS Administration Library*. You can specify more than one URL, in any order. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, trying the next site in the list only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format ***router-name_log-filename_timestamp***. When you configure file archival by using **archive-states** statement, the transfer file utility uses the default routing instance to connect to the destination server. If the default routing instance is unable to connect to the destination server, the transfer file utility does not work.

Starting in Junos OS 18.4R1, when you configure file archival by using the **archive-sites** statement, the transfer file utility does not work if you have enabled the management instance.

Configuring Local Backup for Accounting Files

You can configure the router to save a copy of the accounting file locally when the normal transfer of the files to the archive site fails. The file is saved to the **/var/log/pfedBackup** directory of the relevant Routing Engine. You must specify whether only the files from the master Routing Engine are saved or files are saved from both the master Routing Engine and the backup (client) Routing Engine.

> **NOTE:** Files saved to the **/var/log/pfedBackup** directory are always compressed to conserve local storage, regardless of whether the **compress** statement is configured.

To configure local backup in the event of failure:

- Specify local backup and which files are saved.

```
[edit accounting-options file filename]
user@host# set backup-on-failure (master-and-slave | master-only)
```

Disabling this feature deletes the backed-up accounting files from the directory.

> **NOTE:** When you do not configure this option, the file is saved on failure into the local directory specified as the last site in the list of archive sites.

Configuring Files to Be Compressed

By default, accounting files are transferred in an uncompressed format. To conserve resources during transmission and on the archive site, you can configure compression for the files.

> **NOTE:** Files saved to the **/var/log/pfedBackup** directory are always compressed to conserve local storage, regardless of whether the **compress** statement is configured.

To configure the router to compress accounting files when they are transferred:

- Specify compression.

```
[edit accounting-options file filename]
user@host# set compress
```

Configuring the Maximum Number of Files

To configure the maximum number of files:

- Specify the number.

```
[edit accounting-options file filename]
user@host# set files number
```

When a log file reaches its maximum size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for ***number*** is 3 and the default value is 10.

Configuring the Storage Location of the File

On J Series Services Routers, the files are stored by default on the compact flash drive. Alternatively, you can configure the files to be stored in the **mfs/var/log** directory (on DRAM) instead of the **cf/var/log** directory (on the compact flash drive).

To configure the storage location on DRAM:

- Specify nonpersistent storage.

```
[edit accounting-options file filename]
user@host# set nonpersistent
```

This feature is useful for minimizing read/write traffic on the router's compact flash drive.

NOTE: If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. We recommend that you back up these files periodically.

Configuring Files to Be Saved After a Change in Mastership

You can configure the router to save the accounting files from the new backup Routing Engine to the new master Routing Engine when a change in mastership occurs. The files are stored in the **/var/log/pfedBackup** directory on the router. The master Routing Engine includes these accounting files with its own current accounting files when it transfers the files from the backup directory to the archive site at the next transfer interval. Configure this option when the new backup Routing Engine is not able to connect to the archive site; for example, when the site is not connected by means of an out-of-band interface or the path to the site is routed through a line card.

To configure the backup Routing Engine files to be saved when mastership changes:

- Specify the backup.

```
[edit accounting-options file filename]
user@host# set push-backup-to-master
```

> **NOTE:** The backup Routing Engine's files on the master Routing Engine are sent at each interval even though the files remain the same. If this is more activity than you want, consider using the **backup-on-failure master-and-slave** statement instead.

Configuring the Start Time for File Transfer

To configure the start time for transferring files:

- Specify the time.

```
[edit accounting-options file filename]
user@host# set start-time YYYY-MM-DD.hh:mm
```

For example, 10:00 a.m. on January 30, 2007 is represented as **2007-01-30.10:00**.

Configuring the Transfer Interval of the File

To configure the interval at which files are transferred:

- Specify the interval.

```
[edit accounting-options file filename]
user@host# set transfer-interval minutes
```

The range for **transfer-interval** is 5 through 2880 minutes. The default is 30 minutes.

TIP:

Junos OS saves the existing log file and creates a new file at the configured transfer intervals irrespective of whether:

- The file has reached the maximum size.
- An archive site is configured.

When you have a relatively small transfer interval configured and if no archive site is configured, data can be lost as Junos OS overwrites the log files when the maximum number of log files is reached. To ensure that the log information is saved for a reasonably long time:

- Configure an archive site to archive the log files every time a new log file is created.
- Configure the maximum value (2880 minutes) for **transfer-interval** so that new files are created less frequently; that is, only when the file exceeds the maximum size limit or once in 2 days.

Release History Table

Release	Description
18.4R1	Starting in Junos OS 18.4R1, when you configure file archival by using the **archive-sites** statement, the transfer file utility does not work if you have enabled the management instance.

RELATED DOCUMENTATION

Accounting Options Overview | **840**

Understanding Device Management Functions in Junos OS | **2**

Accounting Options Configuration | **846**

Configuring the Interface Profile | **864**

Configuring the Filter Profile | **868**

Managing Accounting Files

If you configure SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and SRX4600 devices to capture accounting data in log files, set the location for your accounting files to the DRAM.

The default location for accounting files is the **cfs/var/log** directory on the CompactFlash (CF) card. The **nonpersistent** option minimizes the read/write traffic to your CF card. We recommend that you use the **nonpersistent** option for all accounting files configured on your system.

To store accounting log files in DRAM instead of the CF card:

1. Enter configuration mode in the CLI.

2. Create an accounting data log file in DRAM and replace *filename* with the name of the file.

```
[edit]
user@host# edit accounting-options file filename
```

3. Store accounting log files in the DRAM file.

```
[edit]
user@host# set file filename nonpersistent
```

CAUTION: If log files for accounting data are stored on DRAM, these files are lost when the device reboots. Therefore, we recommend that you back up these files periodically.

NOTE: The CLI **nonpersistent** option is not supported on SRX5000 Series devices.

RELATED DOCUMENTATION

Accounting Options Overview | 840

Configuring the Interface Profile

IN THIS SECTION

- Configuring Fields | 865
- Configuring the File Information | 865
- Configuring Cleared Statistics to be Reported in the Flat File | 865
- Configuring the Interval | 866
- Example: Configuring the Interface Profile | 866

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 or logical interface.

To configure an interface profile, include the **interface-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
interface-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

By default, the Packet Forwarding Engine (PFE) periodically collects the statistics for all interfaces. To improve the performance, you can optionally disable the periodic refresh by including the **periodic-refresh disable** statement at the **[edit accounting-options]** hierarchy level.

Each accounting profile must have a unique ***profile-name***. To apply a profile to a physical or logical interface, include the **accounting-profile** statement at either the **[edit interfaces *interface-name*]** or the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level. You can also apply an accounting profile at the **[edit firewall family *family-type* filter *filter-name*]** hierarchy level. For more information, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

To configure an interface profile, perform the tasks described in the following sections:

Configuring Fields

An interface profile must specify what statistics are collected. 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]
fields {
    field-name;
}
```

Configuring the File Information

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]
file filename;
```

You must specify a **file** statement for the interface profile that has already been configured at the **[edit accounting-options]** hierarchy level.

Configuring Cleared Statistics to be Reported in the Flat File

When you issue the **clear interfaces statistics** command for a logical interface configured to collect accounting statistics, all accounting statistics received on that interface from the Packet Forwarding Engine are cleared. The current values when the command is issued become the new baseline and the statistics counters are reset to zero. The new values, starting from zero, are displayed in the CLI. However, they are not reported that way in the accounting flat file associated with the interface. Instead, the values as reported in the file continue to increment as if the command had not been issued.

You can change this result by including the **allow-clear** statement in the interface profile. In this case, when you issue the **clear interfaces statistics** command, the statistics are reset to zero and reported to the flat file.

To configure reporting of cleared accounting statistics to the flat file, specify reporting:

```
[edit accounting-options interface-profile profile-name]
allow-clear;
```

Configuring the Interval

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]
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.

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

Example: Configuring the Interface Profile

Configure the interface profile:

```
[edit]
accounting-options {
    file if_stats {
        size 40 files 5;
    }
    interface-profile if_profile1 {
        file if_stats;
        interval 30;
        fields {
            input-bytes;
            output-bytes;
            input-packets;
            output-packets;
            input-multicast;
            output-multicast;
        }
    }
    interface-profile if_profile2 {
        file if_stats;
        interval 30;
        fields {
            input-bytes;
```

```
            output-bytes;
            input-packets;
            output-packets;
            input-multicast;
            output-multicast;
        }
    }
    interfaces {
        xe-1/0/0 {
            accounting-profile if_profile1;
            unit 0 {
                accounting-profile if_profile2;
                ...
            }
        }
    }
}
```

The two interface profiles, if-profile1 and if-profile2, write data to the same file, if-stats. The if-stats file might look like the following:

```
#FILE CREATED 976823478 2000-12-14-19:51:18
#hostname host
#profile-layout
if_profile2,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets,output-packets,input-multicast,output-multicast
#profile-layout
if_profile1,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets
if_profile2,976823538,xe-1/0/0.0,8,134696815,3681534,501088,40723,0,0
if_profile1,976823538,xe-1/0/0,7,134696815,3681534,501088
...
#FILE CLOSED 976824378 2000-12-14-20:06:18
```

RELATED DOCUMENTATION

- Accounting Options Overview | 840
- Understanding Device Management Functions in Junos OS | 2
- Accounting Options Configuration | 846
- Configuring Accounting-Data Log Files | 856

Configuring the Filter Profile | 868
Configuration Statements at the [edit accounting-options] Hierarchy Level | 844

Configuring the Filter Profile

IN THIS SECTION

- Configuring the Counters | 868
- Configuring the File Information | 869
- Configuring the Interval | 869

A filter profile specifies error and statistics information collected and written to a file. A filter profile must specify counter names for which statistics are collected.

To configure a filter profile, include the **filter-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
filter-profile profile-name {
    counters {
        counter-name;
    }
    file filename;
    interval minutes;
}
```

To apply the filter profile, include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level.

To configure a filter profile, perform the tasks described in the following sections:

Configuring the Counters

Statistics are collected for all counters specified in the filter profile. To configure the counters, include the **counters** statement at the **[edit accounting-options filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]
```

```
counters {
}
```

Configuring the File Information

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 filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]
file filename;
```

You must specify a filename for the filter profile that has already been configured at the **[edit accounting-options]** hierarchy level.

> **NOTE:** The limit on the total number of characters per line in a log file equals 1023. If this limit is exceeded, the output written to the log file is incomplete. Ensure that you limit the number of counters or requested data so that this character limit is not exceeded.

> **NOTE:** If the configured file size or transfer interval is exceeded, Junos OS closes the file and starts a new one. By default, the transfer interval value is 30 minutes. If the transfer interval is not configured, Junos OS closes the file and starts a new one when the file size exceeds its configured value or the default transfer interval value exceeds 30 minutes. To avoid transferring files every 30 minutes, specify a different value for the transfer interval.

Configuring the Interval

Each filter 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 filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]
interval;
```

> **NOTE:** The minimum interval allowed is 1 minute. Configuring a low interval in an accounting profile for a large number of filters might cause serious performance degradation.

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

RELATED DOCUMENTATION

- Accounting Options Overview | 840
- Understanding Device Management Functions in Junos OS | 2
- Accounting Options Configuration | 846
- Configuring Accounting-Data Log Files | 856

Example: Configuring a Filter Profile

Configure a filter profile:

```
[edit]
accounting-options {
    file fw_accounting {
        size 500k files 4;
    }
    filter-profile fw_profile1 {
        file fw_accounting;
        interval 60;
        counters {
            counter1;
            counter2;
            counter3;
        }
    }
}
firewall {
    filter myfilter {
        accounting-profile fw_profile1;
        ...
        term accept-all {
            then {
```

```
            count counter1;
            accept;
        }
    }
  }
}
```

The filter profile, **fw-profile1**, writes data to the file **fw_accounting**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#hostname host
#profile-layout
fw_profile1,epoch-timestamp,filter-name,counter-name,packet-count,byte-count
fw_profile1,976826058,myfilter,counter1,163,10764
...
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

RELATED DOCUMENTATION

Configuring the Filter Profile | 868

Example: Configuring Interface-Specific Firewall Counters and Filter Profiles | 871

Example: Configuring Interface-Specific Firewall Counters and Filter Profiles

To collect and log count statistics collected by firewall filters on a per-interface basis, you must configure a filter profile and include the interface-specific statement at the **[edit firewall filter *filter-name*]** hierarchy level.

Configure the firewall filter accounting profile:

```
[edit accounting-options]
file cust1_accounting {
    size 500k;
}
filter-profile cust1_profile {
    file cust1_accounting;
    interval 1;
    counters {
```

```
        r1;
    }
}
```

Configure the interface-specific firewall counter:

```
[edit firewall]
filter f3 {
    accounting-profile cust1_profile;
    interface-specific;
    term f3-term {
        then {
            count r1;
            accept;
        }
    }
}
```

Apply the firewall filter to an interface:

```
[edit interfaces]
xe-1/0/0 {
    unit 0 {
        family inet {
            filter {
                input f3;
                output f3;
            }
            address 20.20.20.30/24;
        }
    }
}
```

The following example shows the contents of the **cust1_accounting** file in the **/var/log** folder that might result from the preceding configuration:

```
#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
cust1_profile,995495572,xe-1/0/0.0,f3-xe-1/0/0.0-i,r1-xe-1/0/0.0-i,5953,1008257
```

```
cust1_profile,995495602,xe-1/0/0.0,f3-xe-1/0/0.0-o,r1-xe-1/0/0.0-o,5929,1006481
...
```

If the **interface-specific** statement is not included in the configuration, the following output might result:

```
#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
cust1_profile,995495572,xe-1/0/0.0,f3,r1,5953,1008257
cust1_profile,995495632,xe-1/0/0.0,f3,r1,5929,1006481
```

RELATED DOCUMENTATION

Configuring the Filter Profile | 868

Configuring the Interface Profile | 864

Configuring SCU or DCU

IN THIS SECTION

- Creating Prefix Route Filters in a Policy Statement | 874
- Applying the Policy to the Forwarding Table | 874
- Enabling Accounting on Inbound and Outbound Interfaces | 874

To configure SCU or DCU, perform the following tasks described in this section:

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.

Creating Prefix Route Filters in a Policy Statement

To define prefix router filters:

```
[edit policy-options]
policy-statement scu-1 {
    term term1;
    from {
        route-filter 192.0.2.0/24 or longer;
    }
    then source-class gold;
}
```

Applying the Policy to the Forwarding Table

To apply the policy to the forwarding table:

```
[edit]
routing-options {
    forwarding-table {
        export scu-1;
    }
}
```

Enabling Accounting on Inbound and Outbound Interfaces

To enable accounting on inbound and outbound interfaces:

```
[edit]
interfaces {
    so-6/1/0 {
        unit 0 {
            family inet;
            accounting {
                destination-class-usage;
                source-class-usage {
                    output;
                }
            }
        }
    }
}
```

```
[edit]
interfaces {
    xe-0/1/0 {
        unit 0 {
            family inet6 {
                accounting {
                    source-class-usage {
                        input;
                    }
                }
            }
        }
    }
}
```

Optionally, you can include the input and output statements on a single interface as shown:

```
[edit]
interfaces {
    xe-0/1/2 {
        unit 0 {
            family inet6 {
                accounting {
                    source-class-usage {
                        input;
                        output;
                    }
                }
            }
        }
    }
}
```

For more information about configuring route filters and source classes in a routing policy, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide* and the *Junos OS Network Interfaces Library for Routing Devices*.

RELATED DOCUMENTATION

- Understanding Source Class Usage and Destination Class Usage Options | **841**
- Configuring SCU on a Virtual Loopback Tunnel Interface | **876**
- Configuring Class Usage Profiles | **878**

Configuring the MIB Profile | 881
Configuring the Routing Engine Profile | 884

Configuring SCU on a Virtual Loopback Tunnel Interface

IN THIS SECTION

- Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC | 876
- Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface | 877
- Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface | 877

To configure source class usage on the virtual loopback tunnel interface, perform the tasks described in the following sections:

Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC

Define a virtual loop interface on a provider edge router with a Tunnel PIC:

```
[edit interfaces]
vt-0/3/0 {
    unit 0 {
        family inet {
            accounting {
                source-class-usage {
                    input;
                }
            }
        }
    }
}
```

Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface

Map the VRF instance type to the virtual loopback tunnel interface:

```
[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;
      vrf-import import-policy-name;
      vrf-export export-policy-name;
      protocols {
         bgp {
            group to-r4 {
               local-address 10.27.253.1;
               peer-as 400;
               neighbor 10.27.253.2;
            }
         }
      }
   }
}
```

NOTE: For SCU and DCU to work, do not include the **vrf-table-label** statement at the **[edit routing-instances *instance-name*]** hierarchy level.

Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface

Send traffic received from the virtual loopback tunnel interface out of the source class output interface:

```
[edit interfaces]
at-1/1/0 {
   unit 0 {
      family inet {
         accounting {
            source-class-usage {
               output;
```

```
            }
          }
        }
      }
    }
```

For more information about configuring source class usage on the virtual loopback tunnel interface, see the *Junos OS Network Interfaces Library for Routing Devices*.

RELATED DOCUMENTATION

- Understanding Source Class Usage and Destination Class Usage Options | **841**
- Configuring SCU or DCU | **873**
- Configuring Class Usage Profiles | **878**
- Configuring the MIB Profile | **881**
- Configuring the Routing Engine Profile | **884**

Configuring Class Usage Profiles

IN THIS SECTION

- Configuring a Class Usage Profile | **878**
- Configuring the File Information | **879**
- Configuring the Interval | **879**
- Creating a Class Usage Profile to Collect Source Class Usage Statistics | **880**
- Creating a Class Usage Profile to Collect Destination Class Usage Statistics | **880**

To collect class usage statistics, perform the tasks described in these sections:

Configuring a Class Usage Profile

You can configure the class usage profile to collect statistics for particular source and destination classes.

To configure the class usage profile to filter by source classes, include the **source-classes** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]
source-classes {
    source-class-name;
}
```

To configure the class usage profile to filter by destination classes, include the **destination-classes** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]
destination-classes {
    destination-class-name;
}
```

Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To specify which file to use, include the **file** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]
file filename;
```

You must specify a filename for the source class usage profile that has already been configured at the **[edit accounting-options]** hierarchy level. You can also specify a filename for the destination class usage profile configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

Each interface with a class usage profile enabled has statistics collected once per interval 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 class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]
interval;
```

Creating a Class Usage Profile to Collect Source Class Usage Statistics

To create a class usage profile to collect source class usage statistics:

```
[edit]
accounting-options {
    class-usage-profile scu-profile1;
    file usage-stats;
    interval 15;
    source-classes {
        gold;
        silver;
        bronze;
    }
}
```

The class usage profile, **scu-profile1**, writes data to the file **usage_stats**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, scu_profile,epoch-timestamp,interface-name,source-class,
packet-count,byte-count
scu_profile,980313078,xe-1/0/0.0,gold,82,6888
scu_profile,980313078,xe-1/0/0.0,silver,164,13776
scu_profile,980313078,xe-1/0/0.0,bronze,0,0
scu_profile,980313678,xe-1/0/0.0,gold,82,6888
scu_profile,980313678,xe-1/0/0.0,silver,246,20664
scu_profile,980313678,xe-1/0/0.0,bronze,0,0
```

Creating a Class Usage Profile to Collect Destination Class Usage Statistics

To create a class usage profile to collect destination class usage statistics:

```
[edit]
accounting-options {
    class-usage-profile dcu-profile1;
    file usage-stats
    interval 15;
    destination-classes {
        gold;
        silver;
        bronze;
    }
```

```
}
```

The class usage profile, **dcu-profile1**, writes data to the file **usage-stats**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, dcu_profile,epoch-timestamp,interface-name,destination-class,
packet-count,byte-count
dcu_profile,980313078,xe-1/0/0.0,gold,82,6888
dcu_profile,980313078,xe-1/0/0.0,silver,164,13776
dcu_profile,980313078,xe-1/0/0.0,bronze,0,0
dcu_profile,980313678,xe-1/0/0.0,gold,82,6888
dcu_profile,980313678,xe-1/0/0.0,silver,246,20664
dcu_profile,980313678,xe-1/0/0.0,bronze,0,0
...
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

RELATED DOCUMENTATION

- Understanding Source Class Usage and Destination Class Usage Options | **841**
- Configuring SCU or DCU | **873**
- Configuring SCU on a Virtual Loopback Tunnel Interface | **876**
- Configuring the Routing Engine Profile | **884**

Configuring the MIB Profile

IN THIS SECTION

- Configuring the File Information | **882**
- Configuring the Interval | **882**
- Configuring the MIB Operation | **883**
- Configuring MIB Object Names | **883**
- Example: Configuring a MIB Profile | **883**

The MIB profile collects MIB statistics and logs them to a file. The MIB profile specifies the SNMP operation and MIB object names for which statistics are collected.

To configure a MIB profile, include the **mib-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
```

To configure a MIB profile, perform the tasks described in the following sections:

Configuring the File Information

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 mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]
file filename;
```

You must specify a *filename* for the MIB profile that has already been configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

A MIB profile has statistics collected once per interval time specified for the profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]
interval;
```

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

Configuring the MIB Operation

A MIB profile must specify the operation that is used to collect MIB statistics. To configure which operation is used to collect MIB statistics, include the **operation** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]
operation operation-name;
```

You can configure a **get**, **get-next**, or **walk** operation. The default operation is **walk**.

Configuring MIB Object Names

A MIB profile must specify the MIB objects for which statistics are to be collected. To configure the MIB objects for which statistics are collected, include the **objects-names** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]
object-names {
    mib-object-name;
}
```

You can include multiple MIB object names in the configuration.

> **NOTE:** In Junos OS Release 15.1X49-D10 and later, do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Example: Configuring a MIB Profile

Configure a MIB profile:

```
[edit accounting-options]
mib-profile mstatistics {
    file stats;
    interval 60;
    operation walk;
    objects-names {
        ipCidrRouteStatus;
```

```
    }
}
```

Release History Table

Release	Description
15.1X49-D10	In Junos OS Release 15.1X49-D10 and later, do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

RELATED DOCUMENTATION

- Understanding Source Class Usage and Destination Class Usage Options | **841**
- Configuring SCU or DCU | **873**
- Configuring SCU on a Virtual Loopback Tunnel Interface | **876**
- Configuring Class Usage Profiles | **878**
- Configuring the Routing Engine Profile | **884**

Configuring the Routing Engine Profile

IN THIS SECTION

- Configuring Fields | **885**
- Configuring the File Information | **885**
- Configuring the Interval | **886**
- Example: Configuring a Routing Engine Profile | **886**

The Routing Engine profile collects Routing Engine statistics and logs them to a file. The Routing Engine profile specifies the fields for which statistics are collected.

To configure a Routing Engine profile, include the **routing-engine-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

To configure a Routing Engine profile, perform the tasks described in the following sections:

Configuring Fields

A Routing Engine profile must specify what statistics are collected. To configure which statistics should be collected for the Routing Engine, include the **fields** statement at the **[edit accounting-options routing-engine-profile *profile-name*]** hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]
fields {
    field-name;
}
```

Configuring the File Information

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 routing-engine-profile *profile-name*]** hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]
file filename;
```

You must specify a *filename* for the Routing Engine profile that has already been configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

A Routing Engine profile has statistics collected once per interval time specified for the profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options routing-engine-profile *profile-name*]** hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]
interval;
```

The range for **interval** is 1 through 2880 minutes. The default is 30 minutes.

Example: Configuring a Routing Engine Profile

Configure a Routing Engine profile:

```
[edit accounting-options]
file my-file {
    size 300k;
}
routing-engine-profile profile-1 {
    file my-file;
    fields {
        host-name;
        date;
        time-of-day;
        uptime;
        cpu-load-1;
        cpu-load-5;
        cpu-load-15;
    }
}
```

RELATED DOCUMENTATION

- Understanding Source Class Usage and Destination Class Usage Options | **841**
- Configuring SCU or DCU | **873**
- Configuring SCU on a Virtual Loopback Tunnel Interface | **876**
- Configuring Class Usage Profiles | **878**
- Configuring the MIB Profile | **881**

PART 7

Monitoring Options

Configuring Interface Alarms | **888**

Configuring Real-Time Performance Monitoring | **900**

Configuring IP Monitoring | **952**

Configuring sFlow Monitoring Technology | **970**

Packet Flow Accelerator Diagnostics Software | **1006**

CHAPTER 24

Configuring Interface Alarms

IN THIS CHAPTER

- Alarm Overview | 888
- Example: Configuring Interface Alarms | 896

Alarm Overview

IN THIS SECTION

- Alarm Types | 888
- Alarm Severity | 889
- Alarm Conditions | 890

Alarms alert you to conditions on a network interface, on the device chassis, or in the system software that might prevent the device from operating normally. You can set the conditions that trigger alarms on an interface. Chassis and system alarm conditions are preset.

An active alarm lights the **ALARM** LED on the front panel of the device. You can monitor active alarms from the J-Web user interface or the CLI. When an alarm condition triggers an alarm, the device lights the yellow (amber) **ALARM** LED on the front panel. When the condition is corrected, the light turns off.

This section contains the following topics:

Alarm Types

The device supports three types of alarms:

- Interface alarms indicate a problem in the state of the physical links on fixed or installed Physical Interface Modules (PIMs). To enable interface alarms, you must configure them.

- Chassis alarms indicate a failure on the device or one of its components. Chassis alarms are preset and cannot be modified.
- System alarms indicate a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web user interface or CLI.

Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, a new system alarm is introduced to indicate that the PICs (I/O card or SPC) have failed to come online during system start time.

Starting in Junos OS Releases 12.3X48-D85, 15.1X49-D180, and 19.2R1, a system alarm is triggered when the Network Security Process (NSD) is unable to restart due to the failure of one or more NSD subcomponents. The alarm logs about the NSD are saved in the messages log. The alarm is automatically cleared when NSD restarts successfully. The **show chassis alarms** and **show system alarms** commands are updated to display the following output when NSD is unable to restart - **NSD fails to restart because subcomponents fail**.

> **NOTE:** Run the following commands when the CLI prompt indicates that an alarm has been raised:
>
> - **show system alarms**
> - **show chassis alarms**
> - **show chassis fpc pic-status**

For more information about the CLI commands, see **show system alarms**, **show chassis alarms**, and *show chassis fpc (View)*.

Alarm Severity

Alarms have two severity levels:

- Major (red)—Indicates a critical situation on the device that has resulted from one of the following conditions. A red alarm condition requires immediate action.
  - One or more hardware components have failed.
  - One or more hardware components have exceeded temperature thresholds.
  - An alarm condition configured on an interface has triggered a critical warning.
- Minor (yellow)—Indicates a noncritical condition on the device that, if left unchecked, might cause an interruption in service or degradation in performance. A yellow alarm condition requires monitoring or maintenance.

  A missing rescue configuration or software license generates a yellow system alarm.

Alarm Conditions

IN THIS SECTION

- Interface Alarm Conditions | 890
- System Alarm Conditions | 895

To enable alarms on a device interface, you must select an alarm condition and an alarm severity. In contrast, alarm conditions and severity are preconfigured for chassis alarms and system alarms.

> **NOTE:** For information about chassis alarms for your device, see the Hardware Guide for your device.

This section contains the following topics:

Interface Alarm Conditions

Table 80 on page 890 lists the interface conditions, sorted by interface type, that you can configure for an alarm. You can configure each alarm condition to trigger either a major (red) alarm or minor a (yellow) alarm. The corresponding configuration option is included.

For the services stateful firewall filters (NAT, IDP, and IPsec), which operate on an internal adaptive services module within a device, you can configure alarm conditions on the integrated services and services interfaces.

Table 80: Interface Alarm Conditions

Interface	Alarm Condition	Description	Configuration Option
DS1 (T1)	Alarm indication signal (AIS)	The normal T1 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	**ais**
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	**ylw**

Table 80: Interface Alarm Conditions *(continued)*

Interface	Alarm Condition	Description	Configuration Option
Ethernet	Link is down	The physical link is unavailable.	**link-down**
Integrated services	Hardware or software failure	On the adaptive services module, either the hardware associated with the module or the software that drives the module has failed.	**failure**
Serial	Clear-to-send (CTS) signal absent	The remote endpoint of the serial link is not transmitting a CTS signal. The CTS signal must be present before data can be transmitted across a serial link.	**cts-absent**
	Data carrier detect (DCD) signal absent	The remote endpoint of the serial link is not transmitting a DCD signal. Because the DCD signal transmits the state of the device, no signal probably indicates that the remote endpoint of the serial link is unavailable.	**dcd-absent**
	Data set ready (DSR) signal absent	The remote endpoint of the serial link is not transmitting a DSR signal. The DSR signal indicates that the remote endpoint is ready to receive and transmit data across the serial link.	**dsr-absent**
	Loss of receive clock	The clock signal from the remote endpoint is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	**loss-of-rx-clock**
	Loss of transmit clock	The local clock signal is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	**loss-of-tx-clock**

Table 80: Interface Alarm Conditions *(continued)*

Interface	Alarm Condition	Description	Configuration Option
Services	Services module hardware down	A hardware problem has occurred on the device's services module. This error typically means that one or more of the CPUs on the module has failed.	**hw-down**
	Services link down	The link between the device and its services module is unavailable.	**linkdown**
	Services module held in reset	The device's services module is stuck in reset mode. If the services module fails to start up five or more times in a row, the services module is held in reset mode. Startup fails when the amount of time from CPU release to CPU halt is less than 300 seconds.	**pic-hold-reset**
	Services module reset	The device's services module is resetting. The module resets after it crashes or is reset from the CLI, or when it takes longer than 60 seconds to start up.	**pic-reset**
	Services module software down	A software problem has occurred on the device's services module.	**sw-down**

Table 80: Interface Alarm Conditions *(continued)*

Interface	Alarm Condition	Description	Configuration Option
E3	Alarm indication signal (AIS)	The normal E3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	**ais**
	Loss of signal (LOS)	No remote E3 signal is being received at the E3 interface.	**los**
	Out of frame (OOF)	An OOF condition has existed for 10 seconds. This alarm applies only to E3 interfaces configured in frame mode. The OOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds.	**oof**
	Remote defect indication	An AIS, LOS, or OOF condition exists. This alarm applies only to E3 interfaces configured in frame mode.	**rdi**

Table 80: Interface Alarm Conditions *(continued)*

Interface	Alarm Condition	Description	Configuration Option
T3 (DS3)	Alarm indication signal	The normal T3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	**ais**
	Excessive number of zeros	The bit stream received from the upstream host has more consecutive zeros than are allowed in a T3 frame.	**exz**
	Far-end receive failure (FERF)	The remote endpoint of the connection has failed. A FERF differs from a yellow alarm, because the failure can be any failure, not just an OOF or LOS failure.	**ferf**
	Idle alarm	The Idle signal is being received from the remote endpoint.	**idle**
	Line code violation	Either the line encoding along the T3 link is corrupted or a mismatch between the encoding at the local and remote endpoints of a T3 connection occurred.	**lcv**
	Loss of frame (LOF)	An OOF or loss-of-signal LOS condition has existed for 10 seconds. The LOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds. A LOF failure is also called a red failure.	**lof**
	Loss of signal (LOS)	No remote T3 signal is being received at the T3 interface.	**los**
	Phase-locked loop out of lock	The clocking signals for the local and remote endpoints no longer operate in lock-step.	**pll**
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	**ylw**

System Alarm Conditions

Table 81 on page 895 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 81: System Alarm Conditions and Corrective Actions

Alarm Type	Alarm Condition	Corrective Action
Configuration	The rescue configuration is not set.	Set the rescue configuration.
License	You have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed. **NOTE:** This alarm indicates that you are in violation of the software license agreement. You must install a valid license key to be in compliance with all agreements.	Install a valid license key.

Release History Table

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, a new system alarm is introduced to indicate that the PICs (I/O card or SPC) have failed to come online during system start time.
12.3X48-D85 15.1X49-D180 19.2R1	Starting in Junos OS Releases 12.3X48-D85, 15.1X49-D180, and 19.2R1, a system alarm is triggered when the Network Security Process (NSD) is unable to restart due to the failure of one or more NSD subcomponents. The alarm logs about the NSD are saved in the messages log. The alarm is automatically cleared when NSD restarts successfully. The **show chassis alarms** and **show system alarms** commands are updated to display the following output when NSD is unable to restart - **NSD fails to restart because subcomponents fail**.

RELATED DOCUMENTATION

Example: Configuring Interface Alarms | 896

Monitoring Active Alarms on a Device

Monitoring Alarms

System Log Messages

Example: Configuring Interface Alarms

IN THIS SECTION

- Requirements | 896
- Overview | 896
- Configuration | 897
- Verification | 899

This example shows how to configure interface alarms.

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See Interfaces User Guide for Security Devices.
- Select the network interface on which to apply an alarm and the condition you want to trigger the alarm. See “Alarm Overview” on page 888.

Overview

In this example, you enable interface alarms by explicitly setting alarm conditions. You configure the system to generate a red interface alarm when a yellow alarm is detected on a DS1 link. You configure the system to generate a red interface alarm when a link-down failure is detected on an Ethernet link.

For a serial link, you set cts-absent and dcd-absent to yellow to signify either the CST or the DCD signal is not detected. You set loss-of-rx-clock and loss-of-tx-clock to red alarm to signify either the receiver clock signal or the transmission clock signal is not detected.

For a T3 link, you set the interface alarm to red when the remote endpoint is experiencing a failure. You set exz to yellow alarm when the upstream bit has more consecutive zeros than are permitted in a T3 interface. You then set a red alarm when there is loss-of-signal on the interface.

Finally, you configure the system to display active system alarms whenever a user with the login class admin logs in to the device.

Configuration

CLI Quick Configuration

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

```
set chassis alarm ds1 ylw red
set chassis alarm ethernet link-down red
set chassis alarm serial cts-absent yellow dcd-absent yellow
set chassis alarm serial loss-of-rx-clock red loss-of-tx-clock red
set chassis alarm t3 ylw red exz yellow los red
set system login class admin login-alarms
```

Step-by-Step Procedure

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

To configure interface alarms:

1. Configure an alarm.

   ```
   [edit]
   user@host# edit chassis alarm
   ```

2. Specify the interface alarms on a DS1 and an Ethernet link.

   ```
   [edit chassis alarm]
   user@host# set ds1 ylw red
   user@host# set ethernet link–down red
   ```

3. Specify the interface alarms on a serial link.

   ```
   [edit chassis alarm]
   user@host# set serial cts-absent yellow
   user@host# set serial dcd-absent yellow
   user@host# set serial loss-of-rx-clock red
   user@host# set serial loss-of-tx-clock red
   ```

4. Specify the interface alarms on a T3 link.

```
[edit chassis alarm]
user@host# set t3 ylw red
user@host# set t3 exz yellow
user@host# set t3 los red
```

5. Configure the system to display active system alarms.

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

Results

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

```
[edit]
   user@host# show chassis alarms
   t3 {
   exz yellow;
      los red;
   ylw red;
   }
   ds1 {
      ylw red;
   }
   ethernet {
      link-down red;
   }
   serial {
      loss-of-rx-clock red;
      loss-of-tx-clock red;
      dcd-absent yellow;
      cts-absent yellow;
   }
   [edit]
      user@host# show system login
      show system login
   show system login
}
```

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

Verification

Verifying the Alarm Configurations

Purpose

Confirm that the configuration is working properly.

Verify that the alarms are configured.

Action

From configuration mode, enter the **show chassis alarms** command. Verify that the output shows the intended configuration of the alarms.

RELATED DOCUMENTATION

Alarm Overview | 888

Monitoring Active Alarms on a Device

Monitoring Alarms

CHAPTER 25

Configuring Real-Time Performance Monitoring

IN THIS CHAPTER

- RPM Overview | 900
- Understanding Real-Time Performance Monitoring on Switches | 906
- RPM Support for VPN Routing and Forwarding | 910
- RPM Configuration Options | 911
- Two-Way Active Measurement Protocol (TWAMP) Overview | 917
- Example: Configuring TWAMP Client and Server | 919
- Guidelines for Configuring RPM Probes for IPv6 | 926
- Configuring the Interface for RPM Timestamping for Client/Server on a Switch (CLI Procedure) | 927
- Directing RPM Probes to Select BGP Devices | 930
- IPv6 RPM Probes | 930
- Configuring IPv6 RPM Probes | 931
- Tuning RPM Probes | 932
- Monitoring RPM Probes | 933
- Example: Configuring Basic RPM Probes | 937
- Example: Configuring RPM Using TCP and UDP Probes | 944
- Example: Configuring RPM Probes for BGP Monitoring | 948

RPM Overview

IN THIS SECTION

- RPM Probes | 901
- RPM Tests | 902
- Probe and Test Intervals | 902
- Jitter Measurement with Hardware Timestamping | 902
- RPM Statistics | 903

RPM Thresholds and Traps | 904
RPM for BGP Monitoring | 905

The real-time performance monitoring (RPM) feature allows network operators and their customers to accurately measure the performance between two network endpoints. With the RPM tool, you configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter.

RPM allows you to perform service-level monitoring. When RPM is configured on a device, the device calculates network performance based on packet response time, jitter, and packet loss. These values are gathered by Hypertext Transfer Protocol (HTTP) GET requests, Internet Control Message Protocol (ICMP) requests, and TCP and UDP requests, depending on the configuration.

This section contains the following topics:

RPM Probes

You gather RPM statistics by sending out probes to a specified probe target, identified by an IP address or URL. When the target receives the probe, it generates responses, which are received by the device. By analyzing the transit times to and from the remote server, the device can determine network performance statistics.

The device sends out the following probe types:

- HTTP GET request at a target URL
- HTTP GET request for metadata at a target URL
- ICMP echo request to a target address (the default)
- ICMP timestamp request to a target address
- UDP ping packets to a target device
- UDP timestamp requests to a target address
- TCP ping packets to a target device

UDP and TCP probe types require that the remote server be configured as an RPM receiver so that it generates responses to the probes.

The RPM probe results are also available in the form of MIB objects through the SNMP protocol.

NOTE: On SRX300, SRX320, SRX340, SRX1500, SRX4600 devices and vSRX instances, when you configure basic RPM probes, the following combination of the configuration parameters is not supported:

Source address and destination port and next-hop.

Configuring RPM probe with these parameters prevents sending out RPM probes to a specified probe target. We recommend you to configure either the source address or destination port and next-hop to configure RPM probe.

RPM Tests

Each probed target is monitored over the course of a test. A test represents a collection of probes, sent out at regular intervals, as defined in the configuration. Statistics are then returned for each test. Because a test is a collection of probes that have been monitored over some amount of time, test statistics such as standard deviation and jitter can be calculated and included with the average probe statistics.

Probe and Test Intervals

Within a test, RPM probes are sent at regular intervals, configured in seconds. When the total number of probes has been sent and the corresponding responses received, the test is complete. You can manually set the probe interval for each test to control how the RPM test is conducted.

After all the probes for a particular test have been sent, the test begins again. The time between tests is the test interval. You can manually set the test interval to tune RPM performance.

NOTE: On SRX340 devices, the RPM server operation with icmp is not supported. The RPM server works fine with TCP and UDP.

Jitter Measurement with Hardware Timestamping

Jitter is the difference in relative transit time between two consecutive probes.

You can timestamp the following RPM probes to improve the measurement of latency or jitter:

- ICMP ping
- ICMP ping timestamp

- UDP ping
- UDP ping timestamp

> **NOTE:** The device supports hardware timestamping of UDP ping and UDP ping timestamp RPM probes only if the destination port is UDP-ECHO (port 7).

Timestamping takes place during the forwarding process of the device originating the probe (the RPM client), but not on the remote device that is the target of the probe (the RPM server).

The supported encapsulations on a device for timestamping are Ethernet including VLAN, synchronous PPP, and Frame Relay. The only logical interface supported is an **lt** services interface.

RPM probe generation with hardware timestamp can be retrieved through the SNMP protocol.

RPM Statistics

At the end of each test, the device collects the statistics for packet round-trip time, packet inbound and outbound times (for ICMP timestamp probes only), and probe loss as shown in Table 82 on page 903.

Table 82: RPM Statistics

RPM Statistics	Description
Round-Trip Times	
Minimum round-trip time	Shortest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test
Maximum round-trip time	Longest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test
Average round-trip time	Average round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test
Standard deviation round-trip time	Standard deviation of the round-trip times from the Juniper Networks device to the remote server, as measured over the course of the test
Jitter	Difference between the maximum and minimum round-trip times, as measured over the course of the test
Inbound and Outbound Times (ICMP Timestamp Probes Only)	
Minimum egress time	Shortest one-way time from the Juniper Networks device to the remote server, as measured over the course of the test

Table 82: RPM Statistics *(continued)*

RPM Statistics	Description
Maximum ingress time	Shortest one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Average egress time	Average one-way time from the Juniper Networks device to the remote server, as measured over the course of the test
Average ingress time	Average one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Standard deviation egress time	Standard deviation of the one-way times from the Juniper Networks device to the remote server, as measured over the course of the test
Standard deviation ingress time	Standard deviation of the one-way times from the remote server to the Juniper Networks device, as measured over the course of the test
Egress jitter	Difference between the maximum and minimum outbound times, as measured over the course of the test
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
Probe Counts	
Probes sent	Total number of probes sent over the course of the test
Probe responses received	Total number of probe responses received over the course of the test
Loss percentage	Percentage of probes sent for which a response was not received

RPM Thresholds and Traps

You can configure RPM threshold values for the round-trip times, ingress (inbound) times, and egress (outbound) times that are measured for each probe, as well as for the standard deviation and jitter values that are measured for each test. Additionally, you can configure threshold values for the number of successive lost probes within a test and the total number of lost probes within a test.

If the result of a probe or test exceeds any threshold, the device generates a system log message and sends any Simple Network Management Protocol (SNMP) notifications (traps) that you have configured.

Starting in Junos OS Release 18.4R1, if the result of a probe or test exceeds the packet loss threshold, the real-time performance monitoring (RPM) test probe is marked as failed. The test probe also fails when the

round-trip time (RTT) exceeds the configured threshold value. As a result, the device generates an SNMP notification (trap) and marks the RPM test as failed.
RPM allows you to perform service-level monitoring. When RPM is configured on a device, the device calculates network performance based on packet response time, jitter, and packet loss.

RPM for BGP Monitoring

When managing peering networks that are connected using Border Gateway Protocol (BGP), you might need to find out if a path exists between the Juniper Networks device and its configured BGP neighbors. You can ping each BGP neighbor manually to determine the connection status, but this method is not practical when the device has a large number of BGP neighbors configured.

In the device, you can configure RPM probes to monitor the BGP neighbors and determine if they are active.

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1, if the result of a probe or test exceeds the packet loss threshold, the real-time performance monitoring (RPM) test probe is marked as failed. The test probe also fails when the round-trip time (RTT) exceeds the configured threshold value. As a result, the device generates an SNMP notification (trap) and marks the RPM test as failed. RPM allows you to perform service-level monitoring. When RPM is configured on a device, the device calculates network performance based on packet response time, jitter, and packet loss.

RELATED DOCUMENTATION

RPM Configuration Options | **911**

RPM Support for VPN Routing and Forwarding | **910**

Example: Configuring Basic RPM Probes | **937**

Monitoring RPM Probes | **933**

Determine What Causes Jitter and Latency on the Multilink Bundle

Understanding Real-Time Performance Monitoring on Switches

IN THIS SECTION

- RPM Packet Collection | 906
- Tests and Probe Types | 907
- Hardware Timestamps | 907
- Limitations of RPM on EX Series and QFX Series Switches | 909

Real-time performance monitoring (RPM) enables you to configure active probes to track and monitor traffic across the network and to investigate network problems. You can use RPM with Juniper Networks EX Series and QFX Series switches.

The ways in which you can use RPM include:

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
- Set thresholds to trigger SNMP traps when values are exceeded.

  You can configure thresholds for round-trip time, ingress or egress delay, standard deviation, jitter, successive lost probes, and total lost probes per test. (SNMP trap results are stored in **pingResultsTable**, **jnxPingResultsTable**, **jnxPingProbeHistoryTable**, and **pingProbeHistoryTable**.)
- Determine automatically whether a path exists between a host router or switch and its configured BGP neighbors. You can view the results of the discovery using an SNMP client.
- Use the history of the most recent 50 probes to analyze trends in your network and predict future needs.

RPM provides MIB support with extensions for RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

This topic includes:

RPM Packet Collection

Probes collect packets per destination and per application, including ping Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets.

Tests and Probe Types

A test can contain multiple probes. The probe type specifies the packet and protocol contents of the probe.

EX Series and QFX Series switches support the following tests and probe types:

> **NOTE:** QFX Series switches do not support hardware-timestamp probes.

- Ping tests:
  - ICMP echo probe
  - ICMP timestamp probe
- HTTP tests:
  - HTTP get probe (not available for BGP RPM services)
  - HTTP get metadata probe
- UDP and TCP tests with user-configured ports:
  - UDP echo probe
  - TCP connection probe
  - UDP timestamp probe

Hardware Timestamps

To account for latency or jitter in the communication of probe messages, you can enable timestamping of the probe packets (hardware timestamps). If hardware timestamps are not configured, timers are generated at the software level that are less accurate than they would have been with hardware timestamps.

> **NOTE:** QFX Series switches do not support hardware timestamps.

> **NOTE:** On the EX4300 switch, RPM timestamping is performed in the software. The RPM probes at the requester and responder devices are timestamped in the Packet Forwarding Engine instead of the Junos OS process (rmpod) that runs on the Routing Engine. This timestamping method is referred to as pseudo-hardware timestamping.

NOTE: EX Series switches support hardware timestamps for UDP and ICMP probes. EX Series switches do not support hardware timestamps for HTTP or TCP probes.

You can timestamp the following RPM probes to improve the measurement of latency or jitter.

- ICMP ping
- ICMP ping timestamp
- UDP ping
- UDP ping timestamp

NOTE: icmp-ping is the default probe type on devices running Junos OS.

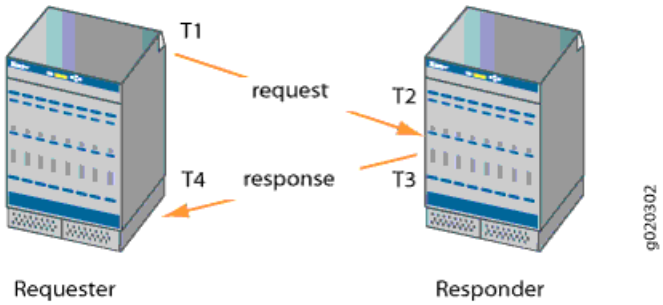
The probe packets are time stamped with the times at which they are sent and received at both the source and destination endpoints.

You should configure the requester (the RPM client) with hardware timestamps (see Figure 34 on page 908) to get more meaningful results than you would get without the timestamps. The responder (the RPM server) does not need to be configured to support hardware timestamps. If the responder supports hardware timestamps, it timestamps the RPM probes. If the responder does not support hardware timestamps, RPM can only report round-trip measurements that include the processing time on the responder.

NOTE: On the EX4300 switch, you must configure the switch as both the requester (the RPM client) and the responder (the RPM server) to timestamp the RPM packet.

Figure 34 on page 908 shows the timestamps:

Figure 34: RPM Timestamps



- T1 is the time the packet leaves the requester port.
- T2 is the time the responder receives the packet.
- T3 is the time the responder sends the response.
- T4 is the time the requester receives the response.

The round-trip time is (T2 – T1) + (T4 – T3). If the responder does not support hardware timestamps, then the round-trip time is (T4 – T1) / 2, and thus includes the processing time of the responder.

You can use RPM probes to find the following time measurements:

- Minimum round-trip time
- Maximum round-trip time
- Average round-trip time
- Standard deviation of the round-trip time
- Jitter of the round-trip time—Difference between the minimum and maximum round-trip time

The RPM feature provides a configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way time, rather than round-trip times, for packets to traverse the network between the requester and the responder. As shown in Figure 34 on page 908, one-way timestamps represent the time T2 – T1 and the time from T4 – T3. Use one-way timestamps when you want to gather information about delay in each direction and to find egress and ingress jitter values.

> **NOTE:** For correct one-way measurement, the clocks of the requester and responder must be synchronized. If the clocks are not synchronized, one-way jitter measurements and calculations can include significant variations, in some cases orders of magnitude greater than the round-trip times.

When you enable one-way timestamps in a probe, the following one-way measurements are reported:

- Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times
- Number of probes sent
- Number of probe responses received
- Percentage of lost probes

Limitations of RPM on EX Series and QFX Series Switches

- Two-Way Active Measurement Protocol (TWAMP) is not supported on the switches.

- The switches do not support user-configured class-of-service (CoS) classifiers or prioritization of RPM packets over regular data packets received on an input interface.
- Timestamps:
  - If the responder does not support hardware timestamps, RPM can only report the round-trip measurements and cannot calculate round-trip jitter.

    NOTE: QFX Series switches do not support hardware timestamps.

  - EX Series switches do not support hardware timestamps or pseudo-hardware timestamps for HTTP and TCP probes.
  - Timestamps apply only to IPv4 traffic.
  - In-Service Software Upgrades (ISSU) and Nonstop Software Upgrades (NSSU) do not support pseudo-hardware timestamps.

RPM Support for VPN Routing and Forwarding

Real-time performance monitoring (RPM) is supported on all Juniper Network devices.

VRF in a Layer 3 VPN implementation allows multiple instances of a routing table to coexist within the same device at the same time. Because the routing instances are independent, the same or overlapping IPv4 or IPv6 addresses can be used without conflicting each other.

RPM ICMP and UDP probe with VPN routing and forwarding (VRF) has been improved. In previous releases, the RPM probes specified to a VRF table were not handled by the real-time forwarding process (FWDD-RT). In Junos OS Release 10.0, RPM probes specified to a VRF table are handled by the FWDD-RT, thereby providing more accurate results.

This feature supports RPM ICMP and UDP probes configured with routing instances of type VRF.

RELATED DOCUMENTATION

RPM Overview | 900

RPM Configuration Options | 911

Monitoring RPM Probes | 933

RPM Configuration Options

You can configure real-time performance monitoring (RPM) parameters. See Table 83 on page 911 for a summary of the configuration options.

Table 83: RPM Configuration Summary

Field	Function	Your Action
Performance Probe Owners		
Owner Name (required)	Identifies an RPM owner for which one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run (a particular customer, for example).	Type the name of the RPM owner.
Identification		
Test name (required)	Uniquely identifies the RPM test	Type the name of the RPM test.
Target (Address or URL) (required)	IPv4 or IPv6 address or URL of probe target	Type the IPv4 address, in dotted decimal notation, IPv6 address, or the URL of the probe target. If the target is a URL, type a fully formed URL that includes **http://**.
Source Address	Explicitly configured IPv4 or IPv6 address to be used as the probe source address	Type the source address to be used for the probe. If the source address is not one of the device's assigned addresses, the packet uses the outgoing interface's address as its source.
Routing Instance	Particular routing instance over which the probe is sent	Type the routing instance name. The routing instance applies only to probes of type **icmp** , **icmp6-ping**, and **icmp-timestamp**. The default routing instance is **inet.0**.
History Size	Number of probe results saved in the probe history	Type a number between 0 and 255. The default history size is 50 probes.
Request Information		

Table 83: RPM Configuration Summary *(continued)*

Field	Function	Your Action
Probe Type (required)	Specifies the type of probe to send as part of the test.	Select the desired probe type from the list: • **http-get** • **http-get-metadata** • **icmp6-ping** • **icmp-ping** • **icmp-ping-timestamp** • **tcp-ping** • **udp-ping**
Interval	Sets the wait time (in seconds) between each probe transmission	Type a number between 1 and 255 (seconds).
Test Interval (required)	Sets the wait time (in seconds) between tests.	Type a number between 0 and 86400 (seconds).
Probe Count	Sets the total number of probes to be sent for each test.	Type a number between 1 and 15.
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks devices configured to receive and transmit RPM probes on the same TCP or UDP port.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6–bit pattern. The default is **000000**.	Type a valid 6–bit pattern.
Data Size	Specifies the size of the data portion of the ICMP probes.	Type a size (in bytes) between 0 and 65507.
Data Fill	Specifies the contents of the data portion of the ICMP probes.	Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.

Table 83: RPM Configuration Summary *(continued)*

Field	Function	Your Action
Hardware Timestamp	Enables timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter: • ICMP ping • ICMP ping timestamp • UDP ping—destination port UDP-ECHO (port 7) only • UDP ping timestamp—destination port UDP-ECHO (port 7) only	To enable timestamping, select the check box.
Maximum Probe Thresholds		
Successive Lost Probes	Sets the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Lost Probes	Sets the total number of probes that must be lost to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Round Trip Time	Sets the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter	Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Sets the total one-way time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).

Table 83: RPM Configuration Summary *(continued)*

Field	Function	Your Action
Ingress Time	Sets the total one-way time (in microseconds), from the remote server to the device, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds)
Jitter Egress Time	Sets the total outbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds)
Jitter Ingress Time	Sets the total inbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Standard Deviation	Sets the maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Ingress Standard Deviation	Sets the maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Traps		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 83: RPM Configuration Summary *(continued)*

Field	Function	Your Action
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates traps when the threshold for maximum inbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates traps when the threshold for jitter in round-trip time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Probe Failure	Generates traps when the threshold for the number of successive lost probes is reached.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
RTT Exceeded	Generates traps when the threshold for maximum round-trip time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Standard Deviation Exceeded	Generates traps when the threshold for standard deviation in round-trip times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Test Completion	Generates traps when a test is completed.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 83: RPM Configuration Summary *(continued)*

Field	Function	Your Action
Test Failure	Generates traps when the threshold for the total number of lost probes is reached.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Performance Probe Server		
TCP Probe Server	Specifies the port on which the device is to receive and transmit TCP probes.	Type the number 7—a standard TCP or UDP port number—or a port number from 49160 through 65535.
UDP Probe Server	Specifies the port on which the device is to receive and transmit UDP probes.	Type the number 7—a standard TCP or UDP port number—or a port number from 49160 through 65535.

NOTE: On SRX300, SRX320, SRX340, SRX1500 devices and vSRX instances, when you configure basic RPM probes, the following combination of the configuration parameters is not supported:

Source address and destination port and next-hop.

Configuring RPM probe with these parameters prevents sending out RPM probes to a specified probe target. We recommend you to configure either the source address or destination port and next-hop to configure RPM probe.

RELATED DOCUMENTATION

RPM Overview | **900**

Example: Configuring Basic RPM Probes | **937**

Example: Configuring RPM Using TCP and UDP Probes | **944**

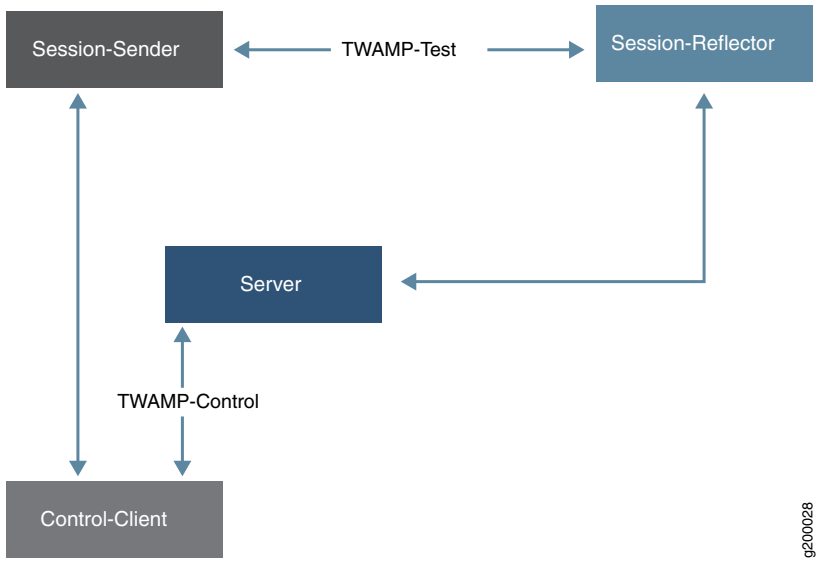
Example: Configuring RPM Probes for BGP Monitoring | **948**

Two-Way Active Measurement Protocol (TWAMP) Overview

The Two-Way Active Measurement Protocol (TWAMP) is an open protocol for measuring network performance between any two devices in a network that supports the protocols in the TWAMP framework. It is a standard protocol framework that separates sessions based on the client/server architecture. The TWAMP client is a host that initiates the TCP connection and acts as a control-client and a session-sender, while the TWAMP server is a host that acknowledges the TCP connection and performs the roles of a server and a session-reflector. TWAMP-Control messages are exchanged between the control-client and the server and TWAMP-Test messages are exchanged between the session-sender and the session-reflector. Four different TWAMP devices can perform the four logical roles of TWAMP control-client, server, session-sender, and session-reflector.

The four elements are shownFigure 35 on page 917.

Figure 35: Four Elements of TWAMP



TWAMP consists of two interrelated protocols –TWAMP-Control and TWAMP-Test. TWAMP- Control is used to initiate, start, and stop test sessions, whereas TWAMP-Test is used to exchange test packets between two TWAMP entities.

- **TWAMP-Control —**A TWAMP control connection is responsible for managing (initiating, starting, and ending) the test sessions between a TWAMP client and a TWAMP server for performance measurement.

  The remote operation process or daemon (rmopd) in the Junos OS Routing Engine takes care of the control plane operations that include handling both the client and server control message exchanges. The packet path processing for the control connection is the same as for any other control process. After the server-greeting, setup-response, and setup-start messages are successfully exchanged, the TWAMP

client starts processing the session creation messages. One or more test sessions are created with the following tuples, that contain:

- Destination IP (DIP) addresses of the client and server
- Source IP (SIP) addresses of the client and server
- UDP ports on the client and server

- **TWAMP-Test —**A TWAMP test session exchanges probe packets to measure the performance metrics. Each test session between a client and server can use different QoS values –for example, round trip time (RTT), delay, and latency variations –to test QoS behavior on the network path for different packet priorities.

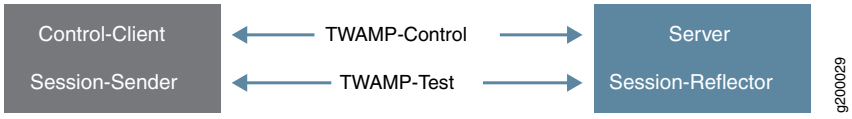
  The timestamps on the test probes on the sender side are just before the packet is sent out on the link. Similarly, timestamps on the test probes on the receiver (server) side are recorded as soon as the probe packets are received from the link. This prompt recording of timestamps helps to calculate fairly accurate RTT, delay, and jitter characteristics of the probes. The test probes can also be set to different QoS values to test the QoS behavior on the network path.

Implementation of TWAMP Elements

A common implementation of TWAMP elements combines the roles of control-client and session-sender in one device (known as the *TWAMP controller* or *TWAMP client*) and the roles of server and session-reflector in the other device (known as the *TWAMP responder* or *TWAMP server*). In this case, each device runs both the TWAMP-Control (between control-client and server) and TWAMP-Test (between session-sender and session-reflector) protocols.

Figure 36 on page 918 illustrates the TWAMP elements, which are implemented as client and server.

Figure 36: The Elements of TWAMP Implemented as Client and Server



Limitations

SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 devices and vSRX instances have the following limitations for TWAMP support:

- TWAMP for IPv6 is not supported.
- TWAMP server and TWAMP client authentication are not supported.

Benefits of TWAMP

- TWAMP configuration helps you activate, test, monitor, and troubleshoot your network end-to-end without using a dedicated testing device.
- TWAMP-Test timestamps provide two-way or round-trip metrics with greater accuracy than other methods (processing delays can be factored as well).
- TWAMP is often used to check service-level agreement (SLA) compliance, and the TWAMP feature is often used in that context.
- Two-way measurements are better than one-way measurements because round-trip delays do not require host clock synchronization. This is possible because the reflector places its own sequence number in the packet.

> **NOTE:** We recommend that you do not configure the RPM client and a TWAMP server on the same device. This might cause some issues in the RPM probe results.

RELATED DOCUMENTATION

Example: Configuring TWAMP Client and Server | 919

Example: Configuring TWAMP Client and Server

IN THIS SECTION

- Requirements | 920
- Overview | 920
- Configuration for TWAMP Client | 921
- Configuration for TWAMP Server | 923
- Verification | 925

This example shows how to configure the Two-Way Active Measurement Protocol (TWAMP) client and TWAMP server.

Requirements

This example uses the following hardware and software components:

- SRX Series device.
- Junos OS Release 18.1R1 and later releases.

Before you begin configuring TWAMP client and TWAMP server, ensure that you have read "Two-Way Active Measurement Protocol (TWAMP) Overview" on page 917 to understand how this task fits into the overall configuration process.

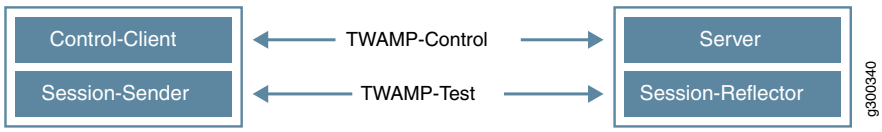
Overview

The TWAMP is an open protocol for measuring network performance between any two devices in a network that supports the TWAMP protocol. The TWAMP consists of TWAMP-Control protocol and TWAMP-Test protocol. The TWAMP-Control protocol is used to initiate, start and stop the test sessions between the control client. The TWAMP-Test protocol used to exchange the test packets between the session sender and the session reflector.

Figure 37 on page 920 shows the TWAMP architecture composed of the following entities that are responsible for starting a monitoring session and exchanging packets:

- The control client initiates all requested test sessions with a start sessions message, and the TWAMP server acknowledges. When necessary, the control client sends a message to stop all test sessions.
- The session sender and the session reflector exchange test packets according to the TWAMP-Test protocol for each active session. On receiving a TWAMP-Test packet, the session reflector reflects a measurement packet and does not collect any packet statistics in TWAMP.

Figure 37: Configuring TWAMP Client and TWAMP Server



The TWAMP server is an end system that manages one or more TWAMP sessions and capable of configuring per-session ports. The TWAMP server listens to the TCP port. The session reflector and TWAMP server make up the TWAMP responder in an IP service-level agreement operation.

For Junos OS Release 18.1R1, both the control client and session sender resides on the same device. The client design does not mandate the TWAMP server and the session reflector to be on the same system. Hence, the Juniper TWAMP client is also capable of working with a third-party server implementation.

Configuration for TWAMP Client

CLI Quick Configuration

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

```
set services rpm twamp client control-connection c1 target-address 10.20.30.1/24
set services rpm twamp client control-connection c1 test-session t1 target-address 10.20.30.2/24
set services rpm twamp client control-connection c1 test-session t1 probe-count 2000
set interfaces ge-0/0/6 unit 0 family inet address 10.20.30.3/24
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/6.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy.

To configure the TWAMP Client:

1. Configure the target address.

   ```
   user@host# set services rpm twamp client control-connection c1 target-address 10.20.30.1/24
   ```

2. Specify the name of the test-session and the target address.

   ```
   user@host# set services rpm twamp client control-connection c1 test-session t1 target-address 10.20.30.2/24
   ```

3. Specify the number of probes within a test.

   ```
   user@host# set services rpm twamp client control-connection c1 test-session t1 probe-count 2000
   ```

4. Set the family inet address.

   ```
   user@host# set interfaces ge-0/0/6 unit 0 family inet address 10.20.30.3/24
   ```

5. Configure zones.

   ```
   user@host# set security zones security-zone trust host-inbound-traffic system-services all
   ```

```
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/6.0
```

Results

From the configuration mode of Router 1, confirm your configuration by entering the **show services rpm twamp**, **show interfaces**, and **show security** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show services rpm twamp
client {
    control-connection c1 {
        target-address 10.20.30.1/24;
        test-session t1 {
            target-address 10.20.30.2/24;
            probe-count 2000;
        }
    }
}
```

```
user@host# show security
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/6.0;
        }
    }
}
```

```
user@host# show interfaces
ge-0/0/6 {
    unit 0 {
        family inet {
            address 10.20.30.3/24;
```

```
    }
  }
}
```

Configuration for TWAMP Server

CLI Quick Configuration

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

```
set services rpm twamp server authentication-mode none
set services rpm twamp server client-list client1 address 10.20.30.4/24
set interfaces ge-0/0/5 unit 0 family inet address 10.20.30.5/24
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/5.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy.

To configure the TWAMP Server:

1. Configure the services and set the authentication mode for the TWAMP server.

   ```
   user@host#set services rpm twamp server authentication-mode none
   ```

2. Specify the client-list name and the address.

   ```
   user@host# set services rpm twamp server client-list client1 address 10.20.30.4/24
   ```

3. Configure the interface and the address.

   ```
   user@host# set interfaces ge-0/0/5 unit 0 family inet address 10.20.30.5/24
   ```

4. Configure zones.

   ```
   user@host# set security zones security-zone trust host-inbound-traffic system-services all
   user@host# set security zones security-zone trust host-inbound-traffic protocols all
   ```

```
user@host# set security zones security-zone trust interfaces ge-0/0/5.0
```

Results

From the configuration mode of Router 1, confirm your configuration by entering the **show services rpm twamp**, **show interfaces**, and **show security** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show services rpm twamp
server {
    authentication-mode none;
    client-list client1 {
        address {
            10.20.30.4/24;
        }
    }
}
```

```
user@host# show security
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/5.0;
        }
    }
}
```

```
user@host# show interfaces
ge-0/0/5 {
    unit 0 {
        family inet {
            address 10.20.30.5/24;
        }
    }
```

```
}
```

Verification

IN THIS SECTION

- Verifying TWAMP Client Sessions | **925**
- Verifying TWAMP Server Sessions | **925**

Confirm that the configuration is working properly.

Verifying TWAMP Client Sessions

Purpose

Verify that the TWAMP client sessions are established.

Action

From operational mode, enter the **show services rpm twamp client session** command.

```
user@host>show services rpm twamp client session
```

```
Connection    Session  Sender          Sender Reflector       Reflector
Name          Name     address         port   address         port
c1            t1       10.20.30.1/24   10001  10.20.30.02/24  10001
```

Verifying TWAMP Server Sessions

Purpose

Verify that the TWAMP server sessions are established.

Action

From operational mode, enter the **show services rpm twamp server session** command.

```
user@host>show services rpm twamp server session
```

```
Session  Connection  Sender          Sender  Reflector       Reflector
ID       ID          address         port    address         port
3        6           10.20.30.4/24   40000   10.20.30.5/24   40000
```

RELATED DOCUMENTATION

Two-Way Active Measurement Protocol (TWAMP) Overview | 917

Guidelines for Configuring RPM Probes for IPv6

Starting with Junos OS Release 15.1X49-D10, you can configure RPM Probes for IPv6.

Keep the following guidelines in mind when you configure IPv6 addresses for RPM destinations or servers:

- IPv6 RPM uses ICMPv6 probe requests. You cannot configure ICMP or ICMP timestamp probe types.
- Only Routing Engine-based RPM is supported for IPv6 targets including VRF support, specification of the size of the data portion of ICMPv6 probes, data pattern, and traffic class.
- You can configure probes with a combination of IPv4 and IPv6 tests. However, an individual test must be either IPv4 or IPv6.
- Routing Engine-based RPM does not support hardware-based, or one-way hardware-based timestamping.
- We recommend that you include the **probe-limit** statement at the **[edit services rpm]** hierarchy level to set the limit on concurrent probes to 10. Higher concurrent probes can result in higher spikes.
- SNMP set operation is permitted only on ICMP probes and it is not supported for other probe types.
- The following table describes the IPv6 special address prefixes that you cannot configure in a probe.

IPV6 Address Type	IPV6 Address Prefix
Node-Scoped Unicast	::1/128 is the loopback address ::/128 is the unspecified address
IPv4-Mapped Addresses	::FFFF:0:0/96
IPv4-Compatible Addresses	:<ipv4-address>/96
Link-Scoped Unicast	fe80::/10
Unique-Local	fc00::/7
Documentation Prefix	2001:db8::/32
6to4	2002::/16
6bone	5f00::/8

IPV6 Address Type	IPV6 Address Prefix
ORCHID	2001:10::/28
Teredo	2001::/32
Default Route	::/0
Multicast	ff00::/8

- In Routing Engine-based RPM, route-trip time (RTT) spikes might occur because of queuing delays, even with a single test.
- Since RPM might open TCP and UDP ports to communicate between the RPM server and RPM client, we recommend that you use firewalls and distributed denial-of-service (DDoS) attack filters to protect against security threats.

RELATED DOCUMENTATION

Configuring IPv6 RPM Probes | 931

Configuring the Interface for RPM Timestamping for Client/Server on a Switch (CLI Procedure)

Use real-time performance monitoring (RPM) to configure active probes to track and monitor traffic across the network and to investigate network problems. To configure basic RPM probes on the EX Series or QFX Series switch, you must configure the probe owner, the test, and the specific parameters of the RPM probe.

You can also set a timestamp to improve the measurement of latency or jitter. The probe is timestamped by the device originating the probe (the RPM client). If you do not enable hardware timestamps, the timer values are set. You should configure both the RPM client (the requester) and the RPM server (the responder) to timestamp the RPM packets. However, if the RPM server does not support hardware timestamps, RPM can only report the round-trip measurements.

NOTE: On the EX4300 switch, RPM timestamping is performed in the software. The RPM probes at the requester and responder devices are timestamped in the Packet Forwarding Engine instead of the Junos OS process (rmpod) that runs on the Routing Engine. This timestamping method is referred to as pseudo-hardware timestamping.

NOTE: QFX Series switches do not support hardware timestamps.

Timestamps apply only to IPv4 traffic.

You can enable hardware timestamps for the following RPM probe types:

- **icmp-ping**
- **icmp-ping-timestamp**
- **udp-ping**
- **udp-ping-timestamp**

To configure RPM probes and to enable hardware timestamping:

1. Specify the probe owner:

   ```
   [edit services rpm]
   user@switch# set probe owner
   ```

2. Specify a test name. A test represents the range of probes over which the standard deviation, average, and jitter are calculated.

   ```
   [edit services rpm probe owner]
   user@switch# set test test-name
   ```

3. Specify the packet and protocol contents of the probe:

   ```
   [edit services rpm probe owner test test-name]
   user@switch# set probe-type type
   ```

4. Specify the destination IPv4 address to be used for the probes:

   ```
   [edit services rpm probe owner test test-name]
   user@switch# set target address
   ```

5. Specify the number of probes within a test:

```
[edit services rpm probe owner test test-name]
user@switch# set probe-count count
```

6. Specify the time, in seconds, to wait between sending packets:

```
[edit services rpm probe owner test test-name]
user@switch# set probe-interval interval
```

7. Specify the time, in seconds, to wait between tests:

```
[edit services rpm probe owner test test-name]
user@switch# set test-interval interval
```

8. Specify the source IP address to be used for probes. If the source IP address is not one of the switch's assigned addresses, the packet uses the outgoing interface's address as its source.

```
[edit services rpm probe owner test test-name]
user@switch# set source-address address
```

9. Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DiffServ code point (DSCP) bits value must be set to a valid 6-bit pattern.

```
[edit services rpm probe owner test test-name]
user@switch# set dscp-code-point dscp-bits
```

10. If you are using ICMP probes, specify the size of the data portion of ICMP probes:

```
[edit services rpm probe owner test test-name]
user@switch# set data-size size
```

11. Enable hardware timestamping of RPM probe messages:

> **NOTE:** QFX Series switches do not support hardware timestamps.

```
[edit services rpm probe owner test test-name]
user@switch# set hardware-timestamp
```

RELATED DOCUMENTATION

Understanding Real-Time Performance Monitoring on Switches | 906

Directing RPM Probes to Select BGP Devices

If a device has a large number of BGP neighbors configured, you can direct (filter) the RPM probes to a selected group of BGP neighbors rather than to all the neighbors. To identify the BGP devices to receive RPM probes, you can configure routing instances.

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

To direct RPM probes to select BGP neighbors:

1. Configure routing instance **RI1** to send RPM probes to BGP neighbors within the routing instance.

```
[edit services rpm bgp]
user@host# set routing-instances RI1
```

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

RELATED DOCUMENTATION

- RPM Overview | **900**
- RPM Configuration Options | **911**
- Example: Configuring Basic RPM Probes | **937**
- Example: Configuring RPM Probes for BGP Monitoring | **948**
- Tuning RPM Probes | **932**

IPv6 RPM Probes

Starting with Junos OS Release 15.1X49-D10, Route Engine-based RPM can send and receive IPv6 probe packets to monitor performance on IPv6 networks.

A probe request is a standard IPv6 packet with corresponding TCP, UDP, and ICMPv6 headers. A probe response is also a standard IPv6 packet with corresponding TCP, UDP, and ICMPv6 headers. No RPM header is appended to the standard packet for RE-based RPM. An IPv6-based RPM test occurs between an IPv6 RPM client and IPv6 RPM server.

NOTE: You can have both IPv4 tests and IPv6 tests in the same probe.

RELATED DOCUMENTATION

Guidelines for Configuring RPM Probes for IPv6 | 926

Configuring IPv6 RPM Probes | 931

Configuring IPv6 RPM Probes

Starting with Junos OS Release 15.1X49-D10, you can configure IPv6 destination addresses for an IPv6-based RPM probe test.

To configure an IPv6 RPM test:

1. Specify the RPM probe owner for the probe you want to configure as an IPv6 test.

```
[edit services rpm]
user@host# edit probe customerA
```

2. Specify a name for the test.

```
[edit services rpm probe customerA]
user@host# edit test ipv6-test
```

3. Specify the probe type.

```
[edit services rpm probe customerA test ipv6-test]
user@host# set probe-type icmp6-ping
```

4. Specify the target address for the test.

```
[edit services rpm probe customerA test ipv6-test]
```

```
user@host# set target inet6-address 2001::2
```

5. Configure the remaining RPM test parameters.

RELATED DOCUMENTATION

Guidelines for Configuring RPM Probes for IPv6 | 926

Tuning RPM Probes

After configuring an RPM probe, you can set parameters to control probe functions, such as the interval between probes, the total number of concurrent probes that a system can handle, and the source address used for each probe packet. See “Example: Configuring Basic RPM Probes” on page 937.

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

To tune RPM probes:

1. Set the maximum number of concurrent probes allowed on the system to **10**.

```
[edit services rpm]
user@host# set probe-limit 10
```

2. Access the ICMP probe of customer A.

```
[edit]
user@host# edit services rpm probe customerA test icmp-test
```

3. Set the time between probe transmissions to 15 seconds.

```
[edit services rpm probe customerA test icmp-test]
user@host# set probe-interval 15
```

4. Set the number of probes within a test to **10**.

```
[edit services rpm probe customerA test icmp-test]
user@host# set probe-count 10
```

5. Set the source address for each probe packet to **192.168.2.9**. If you do not explicitly configure a source address, the address on the outgoing interface through which the probe is sent is used as the source address.

```
[edit services rpm probe customerA test icmp-test]
user@host# set source-address 192.168.2.9
```

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

RELATED DOCUMENTATION

RPM Overview | **900**

RPM Configuration Options | **911**

Example: Configuring RPM Probes for BGP Monitoring | **948**

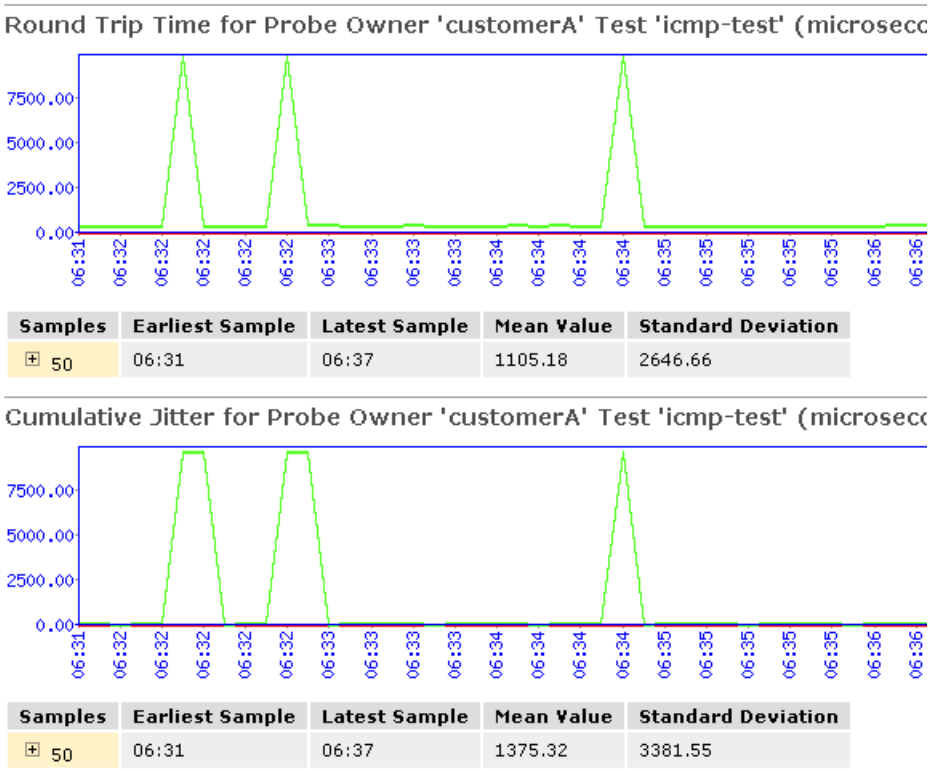
Monitoring RPM Probes

The RPM information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the device. To view these RPM properties, select **Troubleshoot>RPM>View RPM** in the J-Web user interface, or in configuration mode enter the **show** command:

```
[edit]
user@host# run show services rpm probe-results
```

In addition to the RPM statistics for each RPM test, the J-Web user interface displays the round-trip times and cumulative jitter graphically. Figure 38 on page 934 shows sample graphs for an RPM test.

Figure 38: Sample RPM Graphs



In Figure 38 on page 934, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Table 84 on page 934 summarizes key output fields in RPM displays.

Table 84: Summary of Key RPM Output Fields

Field	Values	Additional Information
Currently Running Tests		
Graph		Click the **Graph** link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	–
Test Name	Configured name of the RPM test.	–

Table 84: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Probe Type	Type of RPM probe configured for the specified test: • **http-get** • **http-get-metadata** • **icmp-ping** • **icmp6-ping** • **icmp-ping-timestamp** • **tcp-ping** • **udp-ping**	–
Target Address	IPv4 address, IPv6 address, or URL of the remote server that is being probed by the RPM test.	–
Source Address	Explicitly configured IPv4 or IPv6 source address that is included in the probe packet headers.	If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.	–
Maximum RTT	Longest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.	–
Average RTT	Average round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.	–
Standard Deviation RTT	Standard deviation of round-trip times from the Juniper Networks device to the remote server, as measured over the course of the test.	–
Probes Sent	Total number of probes sent over the course of the test.	–
Loss Percentage	Percentage of probes sent for which a response was not received.	–
Round-Trip Time for a Probe		

Table 84: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Samples	Total number of probes used for the data set.	The Juniper Networks device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	–
Latest Sample	System time when the last probe in the sample was received.	–
Mean Value	Average round-trip time for the 50-probe sample.	–
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	–
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.	–
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	–
Highest Value	Longest round-trip time from the Juniper Networks device to the remote server, as measured over the 50-probe sample.	–
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.	–
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The Juniper Networks device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	–

Table 84: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Latest Sample	System time when the last probe in the sample was received.	–
Mean Value	Average jitter for the 50-probe sample.	–
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.	–
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.	–
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	–
Highest Value	Highest jitter value, as measured over the 50-probe sample.	–
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	–

RELATED DOCUMENTATION

RPM Overview | **900**

RPM Support for VPN Routing and Forwarding | **910**

RPM Configuration Options | **911**

Example: Configuring Basic RPM Probes

IN THIS SECTION

Requirements | **938**

Overview | **938**

Configuration | 939
Verification | 941

This example shows how to configure basic RPM probes to measure performance between two network endpoints.

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces User Guide for Security Devices*.

Overview

In this example, you configure basic probes for two RPM owners, customerA and customerB. You configure the RPM test as icmp-test for customerA with a test interval of 15 seconds and specify a probe type as icmp-ping-timestamp, a probe timestamp, and a target address as 192.178.16.5. You then configure the RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.

Then you configure the RPM test as http-test for customerB with a test interval of 30 seconds and specify a probe type as http-get and a target URL as http://customerB.net. Finally, you configure RPM thresholds and corresponding SNMP traps as probe-failure and test-failure to catch three or more successive lost probes and total lost probes of 10.

NOTE: On SRX300, SRX320, SRX340, SRX1500 devices and vSRX instances, when you configure basic RPM probes, the following combination of the configuration parameters is not supported:

Source address and destination port and next-hop.

Configuring RPM probe with these parameters prevents sending out RPM probes to a specified probe target. We recommend you to configure either the source address or destination port and next-hop to configure RPM probe.

Configuration

CLI Quick Configuration

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

```
set services rpm probe customerA test icmp-test probe-interval 15
set services rpm probe customerA test icmp-test probe-type icmp-ping-timestamp
set services rpm probe customerA test icmp-test hardware-timestamp
set services rpm probe customerA test icmp-test target address 192.178.16.5
set services rpm probe customerA test icmp-test thresholds ingress-time 3000
set services rpm probe customerA test icmp-test traps ingress-time-exceeded
set services rpm probe customerB test http-test probe-interval 30
set services rpm probe customerB test http-test probe-type http-get
set services rpm probe customerB test http-test target url http://customerB.net
set services rpm probe customerB test http-test thresholds successive-loss 3
set services rpm probe customerB test http-test thresholds total-loss 10
set services rpm probe customerB test http-test traps probe-failure
set services rpm probe customerB test http-test traps test-failure
```

Step-by-Step Procedure

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

To configure basic RPM probes:

1. Configure the RPM.

   ```
   [edit]
   user@host# edit services rpm
   ```

2. Configure the RPM owners.

   ```
   [edit services rpm]
   user@host# set probe customerA
   user@host# set probe customerB
   ```

3. Configure the RPM test for customerA.

   ```
   [edit services rpm]
   user@host# edit probe customerA
   ```

```
user@host# set test icmp-test probe-interval 15
user@host# set test icmp-test probe-type icmp-ping-timestamp
```

4. Specify a probe timestamp and a target address.

```
[edit services rpm probe customerA]
user@host# set test icmp-test hardware-timestamp
user@host# set test icmp-test target address 192.178.16.5
```

5. Configure RPM thresholds and corresponding SNMP traps.

```
[edit services rpm probe customerA]
user@host# set test icmp-test thresholds ingress-time 3000
user@host# set test icmp-test traps ingress-time-exceeded
```

6. Configure the RPM test for customerB.

```
[edit]
user@host# edit services rpm probe customerB
user@host# set test http-test probe-interval 30
```

7. Specify a probe type and a target URL.

```
[edit services rpm probe customerB]
user@host# set test http-test probe-type http-get
user@host# set test http-test target url http://customerB.net
```

8. Configure RPM thresholds and corresponding SNMP traps.

```
[edit services rpm probe customerB]
user@host# set test http-test thresholds successive-loss 3
user@host# set test http-test thresholds total-loss 10
user@host# set test http-test traps probe-failure
user@host# set test http-test traps test-failure
```

Results

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

```
[edit]
user@host# show services rpm
probe customerA {
   test icmp-test {
      probe-type icmp-ping-timestamp;
      target address 192.178.16.5;
      probe-interval 15;
      thresholds {
      ingress-time 3000;
      }
         traps ingress-time-exceeded;
         hardware-timestamp;
         }
      }
      probe customerB {
         test http-test {
         probe-type http-get;
         target url http://customerB.net;
         probe-interval 30;
      thresholds {
      successive-loss 3;
         total-loss 10;
         }
            traps [ probe-failure test-failure ];
      }
   }
```

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

Verification

IN THIS SECTION

- Verifying RPM Services | **942**
- Verifying RPM Statistics | **942**

Confirm that the configuration is working properly.

Verifying RPM Services

Purpose

Verify that the RPM configuration is within the expected values.

Action

From operational mode, enter the **show services rpm** command. The output shows the values that are configured for RPM on the device.

Verifying RPM Statistics

Purpose

Verify that the RPM probes are functioning and that the RPM statistics are within expected values.

Action

From configuration mode, enter the **show services rpm probe-results** command.

```
user@host> show services rpm probe-results
```

```
  Owner: customerD, Test: icmp-test
  Probe type: icmp-ping-timestamp
  Minimum Rtt: 312 usec, Maximum Rtt: 385 usec, Average Rtt: 331 usec,
  Jitter Rtt: 73 usec, Stddev Rtt: 27 usec
  Minimum egress time: 0 usec, Maximum egress time: 0 usec,
  Average egress time: 0 usec, Jitter egress time: 0 usec,
  Stddev egress time: 0 usec
  Minimum ingress time: 0 usec, Maximum ingress time: 0 usec,
  Average ingress time: 0 usec, Jitter ingress time: 0 usec,
  Stddev ingress time: 0 usec
  Probes sent: 5, Probes received: 5, Loss percentage: 0

  Owner: customerE, Test: http-test
  Target address: 192.176.17.4, Target URL: http://customerB.net,
  Probe type: http-get
  Minimum Rtt: 1093 usec, Maximum Rtt: 1372 usec, Average Rtt: 1231 usec,
  Jitter Rtt: 279 usec, Stddev Rtt: 114 usec
  Probes sent: 3, Probes received: 3, Loss percentage: 0

Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
  Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
  Routing Instance Name: LR1/RI1
  Probe results:
```

```
    Response received, Fri Oct 28 05:20:23 2005
    Rtt: 662 usec
  Results over current test:
    Probes sent: 5, Probes received: 5, Loss percentage: 0
    Measurement: Round trip time
      Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
      Jitter: 133 usec, Stddev: 53 usec
  Results over all tests:
    Probes sent: 5, Probes received: 5, Loss percentage: 0
    Measurement: Round trip time
      Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
      Jitter: 133 usec, Stddev: 53 usec
```

Configure the traps you want using the **set services rpm probe p1 test t1 traps** command.

If a trap is triggered, you can view the same in the log file named **messages** using the **show snmp log messages | match rmopd** command.

Possible Option	Set of values
egress-jitter-exceeded	Exceeded jitter in egress time threshold
egress-std-dev-exceeded	Exceeded egress time standard deviation threshold
egress-time-exceeded	Exceeded maximum egress time threshold
ingress-jitter-exceeded	Exceeded jitter in ingress time threshold
ingress-std-dev-exceeded	Exceeded ingress time standard deviation threshold
probe-failure	Successive probe loss threshold reached
rtt-exceeded	Exceeded maximum round trip time threshold
std-dev-exceeded	Exceeded round trip time standard deviation threshold
test-completion	Test completed
test-failure	Total probe loss threshold reached

RELATED DOCUMENTATION

RPM Overview | 900
RPM Configuration Options | 911
Tuning RPM Probes | 932

Example: Configuring RPM Using TCP and UDP Probes

IN THIS SECTION

- Requirements | 944
- Overview | 944
- Configuration | 945
- Verification | 947

This example shows how to configure RPM using TCP and UDP probes.

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces User Guide for Security Devices*.
- Configure the probe owner, the test, and the specific parameters of the RPM probe. See "Example: Configuring Basic RPM Probes" on page 937.

Overview

In this example, you configure both the host (device A) and the remote device (device B) to act as TCP and UDP servers. You configure a probe for customerC, which uses TCP packets. Device B is configured as an RPM server for both TCP and UDP packets, using an lt services interface as the destination interface, and ports 50000 and 50037, respectively.

CAUTION: Use probe classification with caution, because improper configuration can cause packets to be dropped.

Configuration

CLI Quick Configuration

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

```
{device A}
set services rpm probe customerC test tcp-test probe-interval 5
set services rpm probe customerC test tcp-test probe-type tcp-ping
set services rpm probe customerC test tcp-test target address 192.162.45.6
set services rpm probe customerC test tcp-test destination-interface lt-0/0/0
set services rpm probe customerC test tcp-test destination-port 50000
```

```
{device B}
set services rpm probe-server tcp port 50000
set services rpm probe-server udp port 50037
```

Step-by-Step Procedure

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

To configure RPM using TCP and UDP probes:

1. Configure the RPM owner on device A.

   ```
   {device A}
   [edit]
   user@host# edit services rpm
   user@host# set probe customerC
   ```

2. Configure the RPM test.

   ```
   {device A}
   [edit services rpm]
   user@host# edit services rpm probe customerC
   user@host# set test tcp-test probe-interval 5
   ```

3. Set the probe type.

   ```
   {device A}
   ```

```
[edit services rpm probe customerC]
user@host# set test tcp-test probe-type tcp-ping
```

4. Specify the target address.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test target address 192.162.45.6
```

5. Configure the destination interface.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test destination-interface lt-0/0/0
```

6. Configure port 50000 as the TCP port to which the RPM probes are sent.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test destination-port 50000
```

7. Configure device B to act as a TCP server using port 50000.

```
{device B}
[edit]
user@host# edit services rpm
user@host# set probe-server tcp port 50000
```

8. Configure device B to act as a UDP server using port 50037.

```
{device B}
[edit services rpm]
user@host# set probe-server udp port 50037
```

Results

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

```
[edit]
user@host# show services rpm
   probe customerC {
   test tcp-test {
      probe-type tcp-ping;
      target address 192.162.45.6;
      probe-interval 5;
      destination-port 50000;
      destination-interface lt-0/0/0.0;
   }
}
probe-server {
   tcp {
      port 50000;
   }
   udp {
      port 50037;
   }
}
```

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

Verification

Verifying RPM Probe Servers

Purpose

Confirm that the configuration is working properly.

Verify that the device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

Action

From configuration mode, enter the **show services rpm active-servers** command. The output shows a list of the protocols and corresponding ports for which the device is configured as an RPM server.

```
user@host> show services rpm active-servers
```

```
   Protocol: TCP, Port: 50000

   Protocol: UDP, Port: 50037
```

RELATED DOCUMENTATION

- RPM Overview | 900
- RPM Configuration Options | 911
- Example: Configuring Basic RPM Probes | 937
- Example: Configuring RPM Probes for BGP Monitoring | 948
- Tuning RPM Probes | 932

Example: Configuring RPM Probes for BGP Monitoring

IN THIS SECTION

- Requirements | 948
- Overview | 948
- Configuration | 949
- Verification | 951

This example shows how to configure RPM probes to monitor BGP neighbors.

Requirements

Before you begin:

- Configure the BGP parameters under RPM configuration to send RPM probes to BGP neighbors. See "Example: Configuring Basic RPM Probes" on page 937.
- Use TCP or UDP probes by configure both the probe server (Juniper Networks device) and the probe receiver (the remote device) to transmit and receive RPM probes on the same TCP or UDP port. See "Example: Configuring RPM Using TCP and UDP Probes" on page 944.

Overview

In this example, you specify a hexadecimal value that you want to use for the data portion of the RPM probe as ABCD123. (It ranges from 1 through 2048 characters.) You specify the data size of the RPM probe as 1024 bytes. (The value ranges from 0 through 65,507.)

Then you configure destination port 50000 as the TCP port to which the RPM probes are sent. You specify the number of probe results to be saved in the probe history as 25. (It ranges from 0 through 255, and the default is 50.) You set the probe count to 5 and probe interval as 1. (The probe count ranges from 1 through 15, and the default is 1; and the probe interval ranges from 1 through 255, and the default is 3.) You then specify tcp-ping as the type of probe to be sent as part of the test.

Finally, you set the test interval as 60. The value ranges from 0 through 86,400 seconds for the interval between tests.

Configuration

CLI Quick Configuration

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

```
set services rpm bgp data-fill ABCD123 data-size 1024
set services rpm bgp destination-port 50000 history-size 25
set services rpm bgp probe-count 5 probe-interval 1
set services rpm bgp probe-type tcp-ping test-interval 60
```

Step-by-Step Procedure

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

To configure RPM probes to monitor BGP neighbors:

1. Configure the RPM and BGP.

   ```
   [edit]
   user@host# edit services rpm bgp
   ```

2. Specify a hexadecimal value.

   ```
   [edit services rpm bgp]
   user@host# set data-fill ABCD123
   ```

3. Specify the data size of the RPM probe.

   ```
   [edit services rpm bgp]
   user@host# set data-size 1024
   ```

4. Configure the destination port.

```
[edit services rpm bgp]
user@host# set destination-port 50000
```

5. Specify the number of probes.

```
[edit services rpm bgp]
user@host# set history-size 25
```

6. Set the probe count and probe interval.

```
[edit services rpm bgp]
user@host# set probe-count 5 probe-interval 1
```

7. Specify the type of probe.

```
[edit services rpm bgp]
user@host# set probe-type tcp-ping
```

> **NOTE:** If you do not specify the probe type the default ICMP probes are sent.

8. Set the test interval.

```
[edit services rpm bgp]
user@host# set test-interval 60
```

Results

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

```
[edit]
   user@host# show services rpm
   bgp {
   probe-type tcp-ping;
```

```
        probe-count 5;
        probe-interval 1;
        test-interval 60;
        destination-port 50000;
        history-size 25;
        data-size 1024;
      data-fill ABCD123;
  }
```

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

Verification

Verifying RPM Probes for BGP Monitoring

Purpose

Confirm that the configuration is working properly.

Verify that the RPM probes for BGP monitoring is configured.

Action

From configuration mode, enter the **show services rpm** command.

RELATED DOCUMENTATION

- RPM Overview | **900**
- RPM Configuration Options | **911**
- Directing RPM Probes to Select BGP Devices | **930**
- Tuning RPM Probes | **932**

CHAPTER 26

Configuring IP Monitoring

IN THIS CHAPTER

- IP Monitoring Overview | 952
- Understanding IP Monitoring Test Parameters | 953
- Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups | 954
- Example: Configuring IP Monitoring on SRX5000 Series Devices | 955
- Example: Configuring IP Monitoring on SRX Series Devices | 962
- Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring | 966

IP Monitoring Overview

This feature monitors IP on standalone SRX Series devices or a chassis cluster redundant Ethernet (reth) interface. Existing RPM probes are sent to an IP address to check for reachability. The user takes action based on the reachability result. Supported action currently is preferred static route injection to system route table.

The actions supported are:

- Adding or deleting a new static route that has a higher priority (lower preference) value than a route configured through the CLI command **set routing-options static route**
- Defining multiple probe names under the same IP monitoring policy. If any probe fails, the action is taken. If all probes are reachable, the action is reverted
- Configuring multiple tests in one RPM probe. All tests must fail for the RPM probe to be considered unreachable. If at least one test reaches its target, the RPM probe is considered reachable
- Configuring multiple failure thresholds in one RPM test. If one threshold is reached, the test fails. If no thresholds are reached, the test succeeds.
- Specifying the no-preempt option. If the no-preempt option is specified, the policy does not perform preemptive failback when it is in a failover state or when the RPM probe test recovers from a failure.

- Setting preferred metric values. If the preferred metric value is set, during failover, the route is injected with the set preferred metric value.
- Enabling and disabling interfaces.
  - **Interface-Enable**—On a physical or logical interface, when the interface-enable action is configured, the initial state of the interface is disable after startup, and it continues to remain in the disable state as long as the associated RPM probe is in the pass state. When the associated RPM probe fails, the configured physical and logical interfaces are enabled.
  - **Interface-Disable**—On a physical or logical interface, when the interface-disable action is configured, the interface state remains unchanged. When the associated RPM probe fails, the physical and logical interfaces are disabled.

> **NOTE:** Multiple probe names and actions can be defined for the same IP monitoring policy.

RELATED DOCUMENTATION

Understanding IP Monitoring Test Parameters | 953

Understanding IP Monitoring Test Parameters

Each probed target is monitored over the course of a test, which represents a collection of probes during which statistics such as standard deviation and jitter are collected are calculated. During a test, probes are generated and responses collected at a rate defined by the probe interval, the number of seconds between probes.

> **NOTE:** To avoid flap, an action is reverted only at the end of a test cycle. During the test cycle, if no threshold is reached, the action is reverted. Although action-failover takes place based on a predefined condition of a monitored IP, when the condition is reversed, the IP becomes reachable on the original route, and the newly added route is deleted. Recovery is performed only when all RPM probes report the IP as reachable.

Table 85 on page 954 lists the test parameters and its default values:

Table 85: Test Parameters and Default Values

Parameter	Default Value
probe-count	1
probe-interval	3 seconds
test-interval	1 second

Table 86 on page 954 lists the supported threshold and its description:

Table 86: Threshold Supported and Description

Threshold	Description
Successive-Loss	Successive loss count of probes
Total-Loss	Total probe lost count

RELATED DOCUMENTATION

IP Monitoring Overview | 952

Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups

IP monitoring checks the reachability of an upstream device. It is designed to check the end-to-end connectivity of configured IP addresses and allows a redundancy group (RG) to automatically failover when the monitored IP address is not reachable through the redundant Ethernet. Both the primary and secondary devices in the chassis cluster monitor specific IP addresses to determine whether an upstream device in the network is reachable.

A redundant Ethernet interface contains physical interfaces from both the primary and secondary nodes in the SRX Series chassis cluster. In a redundant Ethernet interface, two physical interfaces are configured with each node contributing one physical interface. In a redundant Ethernet interface LAG, more than two physical interfaces are configured in the redundant Ethernet interface.

RELATED DOCUMENTATION

IP Monitoring Overview | 952

Example: Configuring IP Monitoring on SRX5000 Series Devices

IN THIS SECTION

- Requirements | 955
- Overview | 955
- Configuration | 957
- Verification | 959

This example shows how to monitor SRX Series devices with chassis cluster enabled.

Requirements

- You need two SRX5800 Services Gateways with identical hardware configurations, one SRX Series device and one EX8208 Ethernet Switch.
- Physically connect the two SRX5800 devices (back-to-back for the fabric and control ports) and ensure that they are the same models. Configure/add these two devices in a cluster.

Overview

IP address monitoring checks end-to-end reachability of configured IP address and allows a redundancy group to automatically fail over when not reachable through the child link of redundant Ethernet interface (known as a reth) interface. Redundancy groups on both devices in a cluster can be configured to monitor specific IP addresses to determine whether an upstream device in the network is reachable.

When you configure multiple IP addresses on the reth Interface in a chassis cluster setup, IP monitoring uses the first IP address from the list of IP addresses configured for that reth interface on the primary node, and the first IP address from the list of secondary IP addresses configured for that reth interface on the backup node. The first IP address is the one with smallest prefix (netmask).

This example shows how to set up IP monitoring on an SRX Series device.

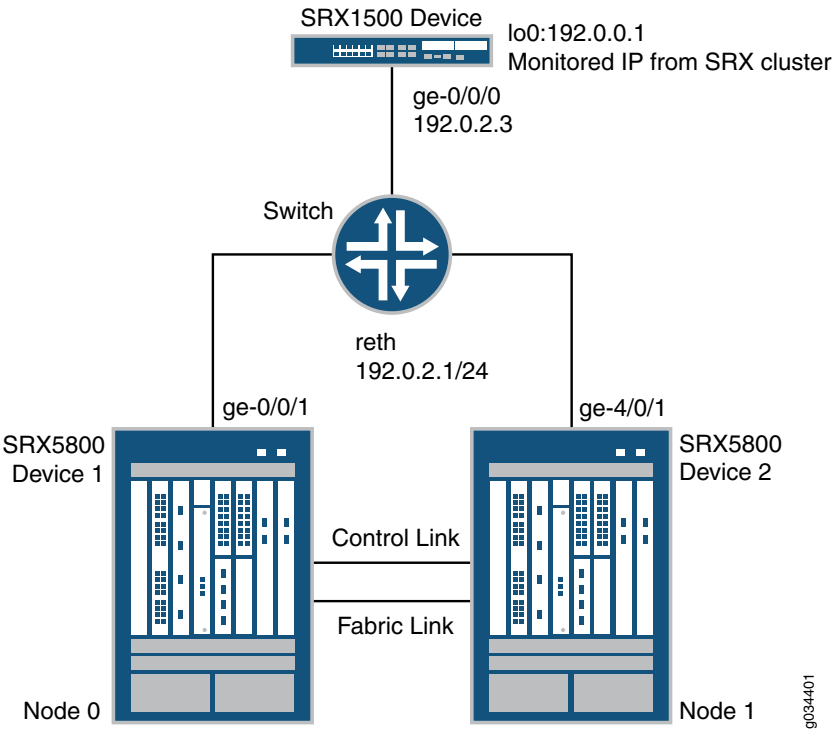
NOTE: IP monitoring is not supported on an NP-IOC card.

NOTE: IP monitoring does not support MIC online/offline status on SRX devices.

Topology

Figure 39 on page 956 shows the topology used in this example.

Figure 39: IP Monitoring on an SRX Series Device Topology Example



In this example, two SRX5800 devices in a chassis cluster are connected to an SRX1500 device through an EX8208 Ethernet Switch. The example shows how the redundancy groups can be configured to monitor key upstream resources reachable through redundant Ethernet interfaces on either node in a cluster.

Configuration

IN THIS SECTION

- Configuring IP Monitoring on SRX Series Device | 957

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 to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set chassis cluster reth-count 1
set chassis cluster redundancy-group 0 node 0 priority 254
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 199
set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1
weight 80
set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1
interface reth0.0 secondary-ip-address 192.0.2.2
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
set interfaces ge-4/0/1 gigether-options redundant-parent reth0
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 192.0.2.1/24
set routing-options static route 192.0.0.1/32 next-hop 192.0.2.3
```

Configuring IP Monitoring on SRX Series Device

Step-by-Step Procedure

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

To configure IP monitoring on an SRX Series device:

1. Specify the number of redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 1
```

2. Specify a redundancy group's priority for primacy on each node of the cluster. The higher number takes precedence.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# set chassis cluster redundancy-group 1 node 0 priority 200
user@host# set chassis cluster redundancy-group 1 node 1 priority 199
```

3. Configure the redundant Ethernet interfaces to redundancy-group 1.

```
{primary:node0}[edit]
user@host# set interfaces reth0 redundant-ether-options redundancy-group 1
user@host# set interfaces reth0 unit 0 family inet address 192.0.2.1/24
```

4. Assign child interfaces for the redundant Ethernet interfaces from node 0 and node 1.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth0
user@host# set interfaces ge-4/0/1 gigether-options redundant-parent reth0
```

5. Configure the static route to the IP address that is to be monitored.

```
{primary:node0}[edit]
user@host# set routing-options static route 192.0.0.1/32 next-hop 192.0.2.3
```

6. Configure IP monitoring under redundancy-group 1 with global weight and global threshold.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
```

```
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80
```

7. Specify the retry interval.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
```

8. Specify the retry count.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

9. Assign a weight to the IP address to be monitored, and configure a secondary IP address that will be used to send ICMP packets from the secondary node to track the IP being monitored.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1 weight 80
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1 interface reth0.0
   secondary-ip-address 192.0.2.2
```

NOTE:

- The redundant Ethernet (reth0) IP address, **192.0.2.1/24**, is used to send ICMP packets from node 0 to check the reachability of the monitored IP.
- The secondary IP address, **192.0.2.2**, should belong to the same network as the reth0 IP address.
- The secondary IP address is used to send ICMP packets from node 1 to check the reachability of the monitored IP.

Verification

IN THIS SECTION

- Verifying Chassis Cluster Status— Before Failover | **960**
- Verifying Chassis Cluster IP Monitoring Status— Before Failover | **960**

Verifying Chassis Cluster Status— After Failover | 961
Verifying Chassis Cluster IP Monitoring Status— After Failover | 961

Confirm the configuration is working properly.

Verifying Chassis Cluster Status— Before Failover

Purpose

Verify the chassis cluster status, failover status, and redundancy group information before failover.

Action

From operational mode, enter the **show chassis cluster status** command.

```
show chassis cluster status
```

```
Cluster ID: 11
Node Priority Status Preempt Manual failover
Redundancy group: 0 , Failover count: 0
node0 254 primary no no
node1 1 secondary no no
Redundancy group: 1 , Failover count: 0
node0 200 primary no no
node1 199 secondary no no
```

Verifying Chassis Cluster IP Monitoring Status— Before Failover

Purpose

Verify the IP status being monitored from both nodes and the failover count for both nodes before failover.

Action

From operational mode, enter the **show chassis cluster ip-monitoring status redundancy-group 1** command.

```
show chassis cluster ip-monitoring status redundancy-group 1
```

```
node0:
--------------------------------------------------------------------------
Redundancy group: 1
```

```
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
node1:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
```

Verifying Chassis Cluster Status— After Failover

Purpose

Verify the chassis cluster status, failover status, and redundancy group information after failover.

> **NOTE:** If the IP address is not reachable, the following output will be displayed.

Action

From operational mode, enter the **show chassis cluster status** command.

```
show chassis cluster status
```

```
Cluster ID: 11
Node Priority Status Preempt Manual failover
Redundancy group: 0 , Failover count: 0
node0 254 primary no no
node1 1 secondary no no
Redundancy group: 1 , Failover count: 1
node0 0 secondary no no
node1 199 primary no no
```

Verifying Chassis Cluster IP Monitoring Status— After Failover

Purpose

Verify the IP status being monitored from both nodes and the failover count for both nodes after failover.

Action

From operational mode, enter the **show chassis cluster ip-monitoring status redundancy-group 1** command.

```
show chassis cluster ip-monitoring status redundancy-group 1
```

```
node0:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 unreachable 1 unknown
node1:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
```

RELATED DOCUMENTATION

Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices

Example: Configuring IP Monitoring on SRX Series Devices

IN THIS SECTION

- Requirements | **962**
- Overview | **963**
- Configuration | **963**
- Verification | **965**

This example shows how to monitor IP on an SRX Series device.

Requirements

Before you begin:

Configure the following RPM options for RPM test:

- target-address
- probe-count

- probe-interval
- test-interval
- thresholds
- next-hop

Overview

This example shows how to set up IP monitoring on an SRX Series device.

Configuration

CLI Quick Configuration

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

```
set services rpm probe Probe-Payment-Server test paysvr target address 1.1.1.10
set services rpm probe Probe-Payment-Server test paysvr probe-count 10
set services rpm probe Probe-Payment-Server test paysvr probe-interval 5
set services rpm probe Probe-Payment-Server test paysvr test-interval 5
set services rpm probe Probe-Payment-Server test paysvr thresholds successive-loss 10
set services rpm probe Probe-Payment-Server test paysvr next-hop 2.2.2.1
set services ip-monitoring policy Payment-Server-Tracking match rpm-probe Probe-Payment-Server
set services ip-monitoring policy Payment-Server-Tracking then preferred-route route 1.1.1.0/24 next-hop
  1.1.1.99
```

Step-by-Step Procedure

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

To configure IP monitoring on an SRX Series Services Gateway:

1. Configure the target address under the RPM probe.

   ```
   [edit ]
   user@host# set services rpm probe Probe-Payment-Server test paysvr target address 1.1.1.10
   ```

2. Configure the probe count under the RPM probe.

   ```
   [edit ]
   ```

```
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-count 10
```

3. Configure the probe interval (in seconds) under the RPM probe.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-interval 5
```

4. Configure the test interval (in seconds) under the RPM probe.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr test-interval 5
```

5. Configure the threshold successive loss count under the RPM

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr thresholds successive-loss 10
```

6. Configure the next-hop IP address under the RPM probe.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr next-hop 2.2.2.1
```

7. Configure the IP monitoring policy under services.

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking match rpm-probe
  Probe-Payment-Server
```

NOTE: The following steps are not mandatory. You can configure interface actions and route actions independently, or you can configure both the interface action and the route action together in one IP monitoring policy.

8. Configure the IP monitoring preferred route under services.

```
[edit ]
```

```
user@host# set services ip-monitoring policy Payment-Server-Tracking then preferred-route route 1.1.1.0/24
  preferred-metric 4
```

9. Configure the IP monitoring interface actions.

   - Enable

     ```
     [edit ]
     user@host# set services ip-monitoring policy Payment-Server-Tracking then interface ge-0/0/1 enable
     ```

   - Disable

     ```
     [edit ]
     user@host# set services ip-monitoring policy Payment-Server-Tracking then interface fe-0/0/[4-6] disable
     ```

10. Configure the no-preempt option.

    ```
    [edit ]
    user@host# set services ip-monitoring policy Payment-Server-Tracking no-preempt
    ```

Verification

Verifying IP Monitoring

Purpose

Verify the IP monitoring status of a policy.

Action

To verify the configuration is working properly, enter the following command:

show services ip-monitoring status *<policy-name>*

RELATED DOCUMENTATION

IP Monitoring Overview | 952

Understanding IP Monitoring Test Parameters | 953

Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring

IN THIS SECTION

- Requirements | 966
- Overview | 966
- Configuration | 967
- Verification | 969

This example shows how to configure redundancy group IP address monitoring for an SRX Series device in a chassis cluster.

Requirements

Before you begin:

- Set the chassis cluster node ID and cluster ID. See *Example: Setting the Node ID and Cluster ID for Security Devices in a Chassis Cluster*
- Configure the chassis cluster management interface. See *Example: Configuring the Chassis Cluster Management Interface*.
- Configure the chassis cluster fabric. See *Example: Configuring the Chassis Cluster Fabric Interfaces*.

Overview

You can configure redundancy groups to monitor upstream resources by pinging specific IP addresses that are reachable through redundant Ethernet interfaces on either node in a cluster. You can also configure global threshold, weight, retry interval, and retry count parameters for a redundancy group. When a monitored IP address becomes unreachable, the weight of that monitored IP address is deducted from the redundancy group IP address monitoring global threshold. When the global threshold reaches 0, the global weight is deducted from the redundancy group threshold. The retry interval determines the ping interval for each IP address monitored by the redundancy group. The pings are sent as soon as the configuration is committed. The retry count sets the number of allowed consecutive ping failures for each IP address monitored by the redundancy group.

In this example, you configure the following settings for redundancy group 1:

- IP address to monitor—10.1.1.10
- IP address monitoring global-weight—100
- IP address monitoring global-threshold—200

  The threshold applies cumulatively to all IP addresses monitored by the redundancy group.
- IP address retry-interval—3 seconds
- IP address retry-count—10
- Weight—100
- Redundant Ethernet interface—reth1.0
- Secondary IP address—10.1.1.101

Configuration

CLI Quick Configuration

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

```
{primary:node0}[edit]
user@host#
set chassis cluster redundancy-group 1 ip-monitoring global-weight 100
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 200
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10 weight 100 interface reth1.0
    secondary-ip-address 10.1.1.101
```

Step-by-Step Procedure

To configure redundancy group IP address monitoring:

1. Specify a global monitoring weight.

   ```
   {primary:node0}[edit]
   user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight 100
   ```

2. Specify the global monitoring threshold.

   ```
   {primary:node0}[edit]
   user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold 200
   ```

3. Specify the retry interval.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
```

4. Specify the retry count.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

5. Specify the IP address to be monitored, weight, redundant Ethernet interface, and secondary IP address.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10 weight 100 interface
   reth1.0 secondary-ip-address 10.1.1.101
```

Results

From configuration mode, confirm your configuration by entering the **show chassis cluster redundancy-group 1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
{primary:node0}[edit]
user@host# show chassis cluster redundancy-group 1
ip-monitoring {
    global-weight 100;
    global-threshold 200;
    family {
        inet {
            10.1.1.10 {
                weight 100;
                interface reth1.0 secondary-ip-address 10.1.1.101;
            }
        }
    }
}
```

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

Verification

Verifying the Status of Monitored IP Addresses for a Redundancy Group

Purpose

Verify the status of monitored IP addresses for a redundancy group.

Action

From operational mode, enter the **show chassis cluster ip-monitoring status** command. For information about a specific group, enter the **show chassis cluster ip-monitoring status redundancy-group** command.

```
{primary:node0}
```

```
user@host> show chassis cluster ip-monitoring status
```

```
node0:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address                Status        Failure count  Reason    Weight
10.1.1.10                 reachable       0            n/a       220
10.1.1.101                reachable       0            n/a       100

node1:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address                Status        Failure count  Reason    Weight
10.1.1.10                 reachable       0            n/a       220
10.1.1.101                reachable       0            n/a       100
```

CHAPTER 27

Configuring sFlow Monitoring Technology

IN THIS CHAPTER

- Overview of sFlow Technology | 970
- Overview of sFlow Technology on ACX Series Routers | 973
- Understanding How to Use sFlow Technology for Network Monitoring | 975
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch | 982
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | 985
- Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | 990
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997
- Example: Monitoring Network Traffic Using sFlow Technology | 999

Overview of sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

sFlow technology implements the following two sampling mechanisms:

- Packet-based sampling—Samples one packet out of a specified number of packets from an interface enabled for sFlow technology. Only the first 128 bytes of each packet are sent to the collector. Data collected include the Ethernet, IP, and TCP headers, along with other application-level headers (if present). Although this type of sampling might not capture infrequent packet flows, the majority of flows are reported over time, allowing the collector to generate a reasonably accurate representation of network activity. You configure packet-based sampling when you specify a sample rate.
- Time-based sampling—Samples interface statistics (counters) at a specified interval from an interface enabled for sFlow technology. Statistics such as Ethernet interface errors are captured. You configure time-based sampling when you specify a polling interval.

An sFlow monitoring system consists of an sFlow agent embedded in the device and up to four external collectors. On a QFX Series standalone switch, the sFlow agent performs packet sampling and gathers interface statistics, and then combines the information into UDP datagrams that are sent to the sFlow collectors. An sFlow collector can be connected to the switch through the management network or data network. The software forwarding infrastructure daemon (SFID) on the switch looks up the next-hop address for the specified collector IP address to determine whether the collector is reachable by way of the management network or data network.

> **NOTE:** On the QFX Series standalone switches, if you configure sFlow technology monitoring on multiple interfaces and a high sampling rate, we recommend that you specify a collector that is on the data network instead of the management network. Having a high volume of sFlow technology monitoring traffic on the management network might interfere with other management interface traffic.

On a QFabric system, the sFlow technology architecture is distributed. The global sFlow technology configuration defined on the QFabric system Director device is distributed to Node groups that have sFlow sampling configured on their interfaces. The sFlow agent has a separate sampling entity, known as a *subagent*, running on each Node device. Each subagent has its own independent state and forwards its own sample information (datagrams) directly to the sFlow collectors.

On the QFabric system, an sFlow collector must be reachable through the data network. Because each Node device has all routes stored in the default routing instance, the collector IP address should be included in the default routing instance to ensure the collector's reachability from the Node device.

Regardless of the rate of traffic or the configured sampling interval, a datagram is sent whenever its size reaches the maximum Ethernet transmission unit (MTU) of 1500 bytes, or whenever a 250-ms timer expires, whichever occurs first. The timer ensures that a collector receives regularly sampled data.

To ensure sampling accuracy and efficiency, QFX Series devices use adaptive sFlow sampling. Adaptive sampling monitors the overall incoming traffic rate on the device and provides feedback to the interfaces to dynamically adapt their sampling rate to traffic conditions. The sFlow agent reads the statistics on the interfaces every 5 seconds and identifies five interfaces with the highest number of samples. On a standalone switch, when the CPU processing limit is reached, a binary backoff algorithm is implemented to reduce the sampling load of the top five interfaces by half. The adapted sampling rate is then to those top five interfaces.

On a QFabric system, sFlow technology monitors the interfaces on each Node device as a group, and implements the binary backoff algorithm based on the traffic on that group of interfaces.

Using adaptive sampling prevents overloading of the CPU and keeps the device operating at its optimum level even when there is a change in traffic patterns on the interfaces. The reduced sampling rate is used until the device is rebooted or when a new sampling rate is configured.

The sFlow collector uses the IP address of the sFlow agent to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID for the sFlow agent remains constant. If you do not assign an IP address to the agent, an IP address will be assigned to the agent using the IP address of a configured interface.

On the QFX Series standalone switches, the following priority is used to determine which interface will be used:

1. Management Ethernet interface me0 IP address
2. Any Layer 3 interface if the me0 IP address is not available

If a particular interface is not configured, the IP address of the next interface in the priority list is used as the IP address for the agent. Once an IP address is assigned to the agent, the agent ID is not modified until the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent.

In addition, you can explicitly configure the IP address for the source data (sFlow datagrams). On the QFX Series standalone switches, if you do not configure that address, the following priority is used:

- Any Layer 3 interface IP address
- The me0 IP address if no Layer 3 interface IP address is available

On the QFabric system, the following default values are used if the optional parameters are not configured:

- Agent ID is the management IP address of the default partition.
- Source IP is the management IP address of the default partition.

In addition, the QFabric system subagent ID (which is included in the sFlow datagrams) is the ID of the Node group from which the datagram is sent to the collector.

> **NOTE:** On QFX5100 standalone switches and the QFX Series Virtual Chassis (with QFX3500 and QFX3600 switches), egress firewall filters are not applied to sFlow sampling packets. On these platforms, the software architecture is different from that on other QFX Series devices, and sFlow packets are sent by the Routing Engine (not the line card on the host) and are not transiting the switch. Egress firewall filters affect data packets that are transiting a switch but do not affect packets sent by the Routing Engine. As a result, sFlow sampling packets are always sent to the sFlow collector.

On the QFX Series, limitations of sFlow traffic sampling include:

- sFlow sampling on ingress interfaces does not capture CPU-bound traffic.
- sFlow sampling on egress interfaces does not support broadcast and multicast packets.
- Egress samples do not contain modifications made to the packet in the egress pipeline.

- If a packet is discarded because of a firewall filter, the reason code for discarding the packet is not sent to the collector.
- The **out-priority** field for a VLAN is always set to 0 (zero) on ingress and egress samples.
- You cannot configure sFlow monitoring on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.

RELATED DOCUMENTATION

Understanding How to Use sFlow Technology for Network Monitoring | **975**

Example: Monitoring Network Traffic Using sFlow Technology | **999**

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

Overview of sFlow Technology on ACX Series Routers

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

An sFlow monitoring system consists of an sFlow agent embedded in the device and a central data collector, or sFlow analyzer. The sFlow agent performs packet sampling and gathers interface statistics, and then combines the information into UDP datagrams that are sent to the sFlow collectors for analysis. The sFlow agent is responsible for monitoring the network port, sample all incoming packets including control traffic and traffic arriving on all the ports in the system. The collector can be connected to one of the data ports or the management interface.

> **NOTE:** sFlow technology is supported only on the ACX5000 line of routers, other ACX Series routers do not support this technology.

The following sFlow features are supported on the ACX5000 line of routers:

- Packet-based sampling—Samples one packet out of a specified number of packets from an interface enabled for sFlow technology. Only the first 128 bytes of each packet are sent to the collector. Data collected include the Ethernet, IP, and TCP headers, along with other application-level headers (if present).

Although this type of sampling might not capture infrequent packet flows, the majority of flows are reported over time, allowing the collector to generate a reasonably accurate representation of network activity. You configure packet-based sampling when you specify a sample rate.

- Time-based sampling—Samples interface statistics (counters) at a specified interval from an interface enabled for sFlow technology. Statistics such as Ethernet interface errors are captured. You configure time-based sampling when you specify a polling interval.
- Adaptive sampling—Monitors the overall incoming traffic rate on the device and provides feedback to the interfaces to dynamically adapt their sampling rate to traffic conditions.

> **NOTE:** If you configure sFlow technology monitoring on multiple interfaces and a high sampling rate, we recommend that you specify a collector that is on the data network instead of the management network. Having a high volume of sFlow technology monitoring traffic on the management network might interfere with other management interface traffic.

The sFlow collector uses the IP address of the sFlow agent to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID for the sFlow agent remains constant. If you do not assign an IP address to the agent, an IP address will be assigned to the agent using the IP address of a configured interface.

If a particular interface is not configured, the IP address of the next interface in the priority list is used as the IP address for the agent. Once an IP address is assigned to the agent, the agent ID is not modified until the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent.

The following sFlow technology limitations apply on ACX5000 line of routers:

- The ingress and egress sampling can be configured only on one of the units under a physical interface and the sFlow is enabled for the physical interface (port). The sFlow cannot be enabled if the unit under a physical interface is not configured.
- Egress sampling for Broadcast, Unknown unicast and Multicast (BUM) traffic is not supported because the **source-interface** field in the SFlow datagrams cannot be populated.
- Destination VLAN and Destination Priority fields are not populated in the case of Layer 3 forwarding.
- SFlow sampling is not supported on the output interface of an analyzer.
- SNMP MIB support for SFlow is not available.
- SFlow cannot be enabled on LAG interfaces, however, it can be enabled on LAG member interfaces individually.
- SFlow cannot be enabled on IRB interfaces.
- SFlow cannot be enabled on logical tunnel (lt-) and LSI interfaces.

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Understanding How to Use sFlow Technology for Network Monitoring

IN THIS SECTION

- Benefits of sFlow Technology | 975
- Sampling Mechanism and Architecture of sFlow Technology | 975
- Adaptive Sampling | 977
- sFlow Agent Address Assignment | 979
- sFlow Limitations on Routers | 980
- sFlow Limitations on Switches | 981

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow randomly samples network packets and sends the samples to a monitoring station called a *collector*.

This topic describes:

Benefits of sFlow Technology

- sFlow can be used by software tools like a network analyzer to continuously monitor tens of thousands of switch or router ports simultaneously.
- Because sFlow uses network sampling (forwarding one packet from *n* number of total packets) for analysis, it is not resource intensive (for example processing, memory and more). The sampling is done at the hardware application-specific integrated circuits (ASICs) and, hence, it is simple and more accurate.

Sampling Mechanism and Architecture of sFlow Technology

sFlow technology uses the following two sampling mechanisms:

- Packet-based sampling—Samples one packet out of a specified number of packets from an interface enabled for sFlow technology. Only the first 128 bytes of each packet are sent to the collector. Data collected include the Ethernet, IP, and TCP headers, along with other application-level headers (if present). Although this type of sampling might not capture infrequent packet flows, the majority of flows are

reported over time, allowing the collector to generate a reasonably accurate representation of network activity. To configure packet-based sampling, you must specify a sample rate.

- Time-based sampling—Samples interface statistics at a specified interval from an interface enabled for sFlow technology. Statistics such as Ethernet interface errors are captured. To configure time-based sampling, you must specify a polling interval.

The sampling information is used to create a network traffic visibility picture. The Juniper Networks Junos operating system (Junos OS) fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks* (see http://faqs.org/rfcs/rfc3176.html).

> **NOTE:** On switches, sFlow technology samples only raw packet headers, that is, the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent embedded in the router or switch and a centralized collector. The sFlow agent's two main activities are random sampling and statistics gathering. It combines interface counters and flow samples and sends them across the network to the sFlow collector as UDP datagrams, directing those datagrams to the IP address and UDP destination port of the collector. Each datagram contains the following information:

- The IP address of the sFlow agent
- The number of samples
- The interface through which the packets entered the agent
- The interface through which the packets exited the agent
- The source and destination interface for the packets
- The source and destination VLAN for the packets

> **CAUTION:** In case of dual VLANs, all fields may not be reported.

Routers and switches can adopt the distributed sFlow architecture. The sFlow agent has subagents. Each subagent is responsible for monitoring a set of network ports and has a unique ID that is used by the collector to identify the data source. A subagent has its own independent state and forwards its own sample messages to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Because sampling is distributed across subagents, the protocol overhead associated with sFlow technology is significantly reduced at the collector.

NOTE: On the QFabric system, an sFlow collector must be reachable through the network. Because each Node device has all routes stored in the default routing instance, the collector IP address should be included in the default routing instance to ensure the collector's reachability from the Node device.

NOTE: You cannot configure sFlow monitoring on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.

Infrequent sampling flows might not be reported in the sFlow information, but over time the majority of flows are reported. Based on a configured sampling rate *N*, 1 out of *N* packets is captured and sent to the collector. This type of sampling does not provide a 100 percent accurate result in the analysis, but it does provide a result with quantifiable accuracy. A user-configured polling interval defines how often sFlow data for a specific interface are sent to the collector, but an sFlow agent can also schedule polling.

NOTE: For the EX9200 switch and MX Series routers, we recommend that you configure the same sample rate for all the ports in a line card. If you configure different sample rates, the lowest value is used for all ports on the line card.

NOTE: If the mastership assignment changes in a Virtual Chassis setup, sFlow technology continues to function.

Adaptive Sampling

Adaptive sampling is the process of monitoring the overall incoming traffic rate on the network device and providing intelligent feedback to interfaces to dynamically adapt the sampling rates on interfaces on the basis of traffic conditions. Adaptive sampling prevents the CPU from overloading and maintains the system at an optimum level, even when traffic patterns change on the interfaces. Whereas the *sample rate* is the configured number of egress or ingress packets out of which one packet is sampled, the *adaptive sample rate* is the maximum number of samples that should be generated per line card, that is, it's the limit given to adaptive sampling. *Sample load* is the amount of data (or number of packets) moving across a network at a given point of time that is sampled. As you increase the sample rate, you decrease the sample load and vice versa. For example, suppose the configured sample rate is 2 (meaning 1 packet out of 2 packets is sampled), and then that rate is doubled, making it 4, or only 1 packet out of 4 packets is sampled.

You configure the adaptive sample rate, which is the maximum number of samples that should be generated per line card, at the **[edit protocols sflow adaptive-sample-rate** hierarchy level.

How Adaptive Sampling Works

Every few seconds, or cycle, the sFlow agent collects the interface statistics. From these aggregated statistics, an average number of samples per second is calculated for the cycle. The cycle length depends on the platform:

- Every 12 seconds for EX Series and QFX5K switches and MX Series and PTX Series routers
- Every 5 seconds for QFX Series switches other than QFX5K

If the combined sample rate of all the interfaces on an line card exceeds the adaptive sample rate, a binary backoff algorithm is initiated, which reduces the sample load on the interfaces. Adaptive sampling doubles the sample rate on the affected interfaces, which reduces the sampling load by half. This process is repeated until the CPU load due to sFlow on a given line card comes down to an acceptable level.

Which interfaces on an line card participate in adaptive sampling depends on the platform:

- For MX Series routers and EX Series switches, the sample rates on all the interfaces on the line card are adapted.
- For PTX Series routers and QFX Series switches, only the five interfaces with the highest sample rates on the line card are adapted.

> **NOTE:**
>
> On a QFabric system, sFlow technology monitors the interfaces on each node device as a group, and implements the binary backoff algorithm based on the traffic on that group of interfaces.

For all platforms, the increased sampling rates remain in effect until one of the following conditions is achieved:

- The device is rebooted.
- A new sample rate is configured.

If you have enabled the adaptive sampling fallback feature and, because of a traffic spike, the number of samples increases to the configured sample-limit-threshold, then the adaptive sampling rate is reversed. See “Adaptive Sampling Fallback” on page 978.

Adaptive Sampling Fallback

The *adaptive sampling fallback* feature, when configured and after adaptive sampling has taken place, uses a binary backup algorithm to decrease the sampling rate (thus, increasing the sampling load) when the number of samples generated is less than the configured **sample-limit-threshold** value, without affecting normal traffic.

Starting in Junos OS Release 18.3R1, for EX Series switches, Junos OS supports the adaptive sampling fallback feature. Starting in Junos OS Release 19.1R1, for MX Series, PTX Series, and QFX Series devices, Junos OS supports the adaptive sampling fallback feature.

Adaptive sampling fallback is disabled by default. To enable this feature, include the **fallback** and **adaptive-sample-rate** ***sample-limit-threshold*** options in the **[edit protocols sflow** adaptive-sample-rate**]** hierarchy level.

After adaptive sampling has taken place and the line card is underperforming—that is, the number of samples generated in a cycle are less than the configured value for the **sample-limit-threshold** statement—for five continuous cycles of adaptive sampling, the adapted rate is reversed. If the reverse adaptation has happened and the number of samples generated in a cycle is less than half of the current adapted rate again (and, therefore, for five continuous cycles), another reverse adaptation can happen.

Reverse adaptation does not occur if the interfaces are already at the configured rate.

Adaptive Sampling Limitations

The following are limitations of the adaptive sample feature:

- On standalone routers or standalone QFX Series switches, if you configure sFlow on multiple interfaces and with a high sampling rate, we recommend that you specify a collector that is on the data network instead of on the management network. Having a high volume of sFlow traffic on the management network might interfere with other management interface traffic.
- On routers, sFlow does not support graceful restart. When a graceful restart occurs, the adaptive sampling rate is set to the user-configured sampling rate.
- On a rate-selectable line card (which supports multiple speeds), interfaces with the highest sample count are selected for adaptive sampling fallback. The backup algorithm selects those interfaces on which the adaptive sampling rate is increased the maximum number of times and then decreases the sampling rate on each of those interfaces every five seconds. However, on a single-rate line card, only one sample rate is supported per line card, and the adaptive sampling fallback mechanism backs up the sampling rate on all the interfaces of the line card.

sFlow Agent Address Assignment

The sFlow collector uses the sFlow agent's IP address to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID of the sFlow agent remains constant.

If you do not specify the IP address to be assigned to the agent, an IP address is automatically assigned to the agent based on the following order of priority of interfaces configured on the device:

Routers and EX Series Switches	QFX Series Devices
1. Virtual Management Ethernet (VME) interface 2. Management Ethernet interface	1. Management Ethernet interface me0 IP address 2. Any Layer 3 interface if the me0 IP address is not available

If a particular interface is not configured, the IP address of the next interface in the priority list is used as the IP address for the agent. Once an IP address is assigned to the agent, the agent ID is not modified until the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent. When the agent's IP address is assigned automatically, the IP address is dynamic and changes when the device reboots.

On the QFabric system, the following default values are used if the optional parameters are not configured:

- Agent ID is the management IP address of the default partition.
- Source IP is the management IP address of the default partition.

In addition, the QFabric system subagent ID (which is included in the sFlow datagrams) is the ID of the node group from which the datagram is sent to the collector.

sFlow data can be used to provide network traffic visibility information. You can explicitly configure the source IP address to be assigned to the sFlow datagrams. If you do not explicitly configure the IP address, the IP address of any of the configured Layer 3 network interfaces is used as the source IP address. If a Layer 3 IP address is not configured, then the agent IP address is used as the source IP address.

sFlow Limitations on Routers

On routers, limitations of sFlow traffic sampling include the following:

- Trio chipset cannot support different sampling rate for each family. Hence, only one sampling rate can be supported per line card.
- Adaptive load balancing is applied per line card and not for per interface under the line card.

Routers support configuration of only one sampling rate (inclusive of ingress and egress rates) on an line card. To support compatibility with the sflow configuration of other Juniper Networks products, the routers still accept multiple rate configuration on different interfaces of the same line card. However, the router programs the lowest rate as the sampling rate for all the interfaces of that line card. The (**show sflow interfaces**) command displays the configured rate and the actual (effective) rate. However, different rates on different line cards is still supported on Juniper Networks routers.

sFlow Limitations on Switches

On the QFX Series, limitations of sFlow traffic sampling include the following:

- sFlow sampling on ingress interfaces does not capture CPU-bound traffic.
- sFlow sampling on egress interfaces does not support broadcast and multicast packets.
- Egress samples do not contain modifications made to the packet in the egress pipeline.
- If a packet is discarded because of a firewall filter, the reason code for discarding the packet is not sent to the collector.
- On EX9200 switches and QFX Series switches except the QFX10K switches, true OIF (outgoing interface) is not supported with sFlow.
- The out-priority field for a VLAN is always set to 0 (zero) on ingress and egress samples.
- On QFX5100 standalone switches and the QFX Series Virtual Chassis (including mixed QFX Series Virtual Chassis), egress firewall filters are not applied to sFlow sampling packets. On these platforms, the software architecture is different from that on other QFX Series devices—sFlow packets are sent by the Routing Engine (not the line card on the host) and do not transit the switch. Egress firewall filters affect data packets that are transiting a switch, but do not affect packets sent by the Routing Engine. As a result, sFlow sampling packets are always sent to the sFlow collector.

EX9200 switches support configuration of only one sampling rate (inclusive of ingress and egress rates) on an FPC (or line card). To support compatibility with the sflow configuration of other Juniper Networks products, EX9200 switches still accept multiple rate configuration on different interfaces of the same FPC. However, the switch programs the lowest rate as the sampling rate for all the interfaces of that FPC. The (**show sflow interfaces**) command displays the configured rate and the actual (effective) rate. However, different rates on different FPCs is still supported on EX9200 switches.

Release History Table

Release	Description
19.1R1	Starting in Junos OS Release 19.1R1, for MX Series, PTX Series, and QFX Series devices, Junos OS supports the adaptive sampling fallback feature.
18.3R1	Starting in Junos OS Release 18.3R1, for EX Series switches, Junos OS supports the adaptive sampling fallback feature.

Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch

IN THIS SECTION

- Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches | 982
- Adaptive Sampling | 983
- sFlow Agent Address Assignment | 984

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station. You can configure sFlow technology on a Juniper Networks EX Series Ethernet Switch to continuously monitor traffic at wire speed on all interfaces simultaneously.

This topic describes:

Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches

sFlow technology uses the following two sampling mechanisms:

- Packet-based sampling: Samples one packet out of a specified number of packets from an interface enabled for sFlow technology.
- Time-based sampling: Samples interface statistics at a specified interval from an interface enabled for sFlow technology.

The sampling information is used to create a network traffic visibility picture. The Juniper Networks Junos operating system (Junos OS) fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

> **NOTE:** sFlow technology on the switches samples only raw packet headers. A raw Ethernet packet is the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent's two main activities are random sampling and statistics gathering. The sFlow agent combines interface counters and flow samples and sends them across the network to the sFlow collector in UDP datagrams, directing those datagrams to the IP address and UDP destination port of the collector. Each datagram contains the following information:

- The IP address of the sFlow agent
- The number of samples
- The interface through which the packets entered the agent
- The interface through which the packets exited the agent
- The source and destination interface for the packets
- The source and destination VLAN for the packets

EX Series switches adopt the distributed sFlow architecture. The sFlow agent has two separate sampling entities that are associated with each Packet Forwarding Engine. These sampling entities are known as subagents. Each subagent has a unique ID that is used by the collector to identify the data source. A subagent has its own independent state and forwards its own sample packets to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Because sampling is distributed across subagents, the protocol overhead associated with sFlow technology is significantly reduced at the collector.

NOTE: You cannot configure sFlow monitoring on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.

NOTE: If the mastership assignment changes in a Virtual Chassis setup, sFlow technology continues to function.

Adaptive Sampling

The switches use adaptive sampling to ensure both sampling accuracy and efficiency. Adaptive sampling is a process of monitoring the overall incoming traffic rate on the network device and providing intelligent feedback to interfaces to dynamically adapt the sampling rates on interfaces on the basis of traffic conditions. Interfaces on which incoming traffic exceeds the system threshold are checked so that all violations can be regulated without affecting the traffic on other interfaces. Every 12 seconds, the agent checks interfaces to get the number of samples, and interfaces are grouped on the basis of the slot that they belong to. The top five interfaces that produce the highest number of samples are selected. Using the binary backoff algorithm, the sampling load on these interfaces is reduced by half and allotted to interfaces that have a lower sampling rate. Therefore, when the processor's sampling limit is reached, the sampling rate is adapted such that it does not load the processor any further. If the switch is rebooted, the adaptive sampling rate is reset to the user-configured sampling rate. Also, if you modify the sampling rate, the adaptive sampling rate changes.

The advantage of adaptive sampling is that the switch continues to operate at its optimum level even when there is a change in the traffic patterns in the interfaces. You do not need to make any changes. Because the sampling rate adapts dynamically to changing network conditions, the resources are utilized optimally resulting in a high-performance network.

Infrequent sampling flows might not be reported in the sFlow information, but over time, the majority of flows are reported. On the basis of the configured sampling rate *N*, 1 out of *N* packets is captured and sent to the collector. This type of sampling does not provide a result that is 100 percent accurate in the analysis, but it does provide a result of quantifiable accuracy. A user-configured polling interval defines how often the sFlow data for a specific interface are sent to the collector, but an sFlow agent can also schedule polling.

> **NOTE:** sFlow technology on EX Series switches does not support graceful restart. When a graceful restart occurs, the adaptive sampling rate is set to the user-configured sampling rate.

sFlow Agent Address Assignment

The sFlow collector uses the sFlow agent's IP address to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID of the sFlow agent remains constant. If you do not configure the IP address of the sFlow agent, an IP address is automatically assigned to the agent. This is the IP address of one of the following interfaces configured on the switch taken in the given order of priority:

1. Virtual management Ethernet (VME) interface

2. Management Ethernet interface

If neither of the preceding interfaces has been configured, the IP address of any Layer 3 interface or the routed VLAN interface (RVI) is assigned to the agent. At least one interface must be configured on the switch for an IP address to be automatically assigned to the agent. When the agent's IP address is assigned automatically, the IP address is dynamic and changes when the switch reboots.

sFlow data can be used to provide network traffic visibility information. You can explicitly configure the IP address to be assigned to source data (sFlow datagrams). If you do not explicitly configure that address, the IP address of the configured Gigabit Ethernet interface, 10-Gigabit Ethernet interface, or the RVI is used as the source IP address.

RELATED DOCUMENTATION

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches

IN THIS SECTION

- Requirements | 985
- Overview and Topology | 985
- Configuration | 986
- Verification | 988

sFlow technology is a networking monitoring technology for high-speed switched or routed networks. It is a technology that is based on statistical sampling. You can configure sFlow technology to continuously monitor traffic at wire speed on all interfaces simultaneously. sFlow data can be used to provide network traffic visibility information. You can specify sampling rates for ingress and egress packets. Junos OS fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

This example describes how to configure and use sFlow technology to monitor network traffic.

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.3 or later for EX Series switches

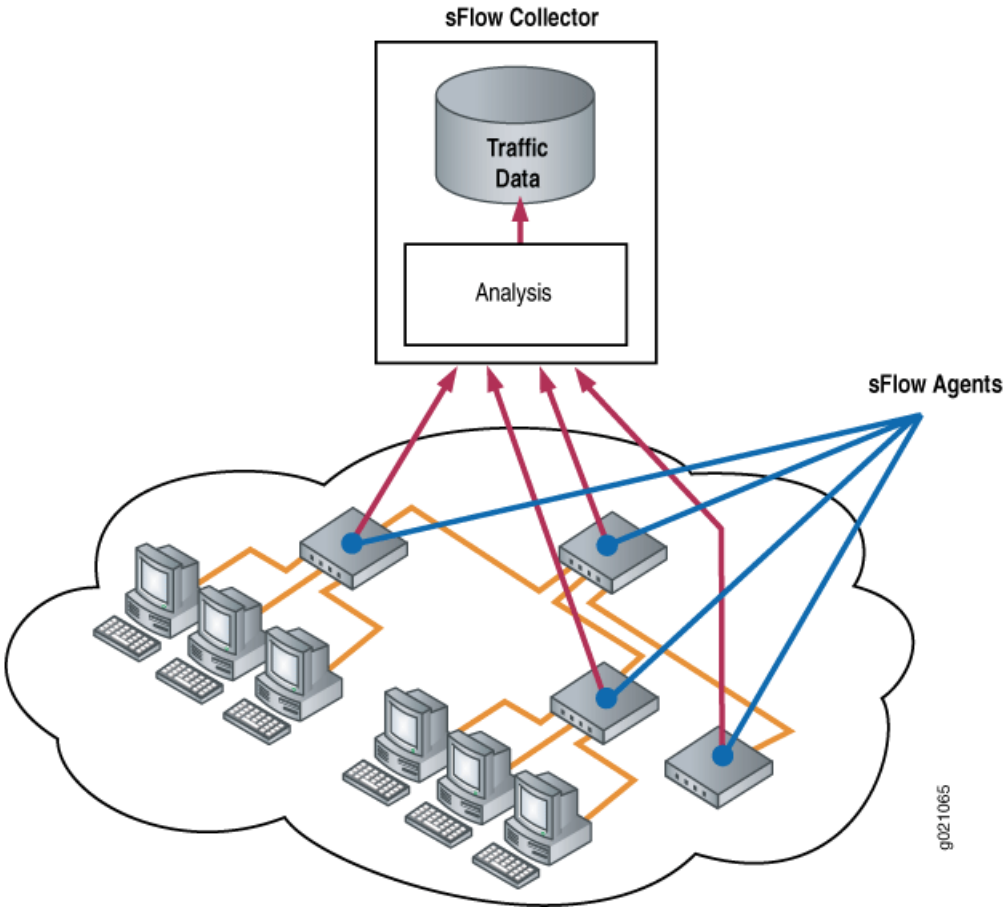
Overview and Topology

sFlow technology samples network packets and sends the samples to a monitoring station. You can specify sampling rates for ingress and egress packets. The information gathered is used to create a network traffic visibility picture.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent runs on the switch. It combines interface counters and flow samples and sends them

across the network to the sFlow collector. Figure 40 on page 986 depicts the basic elements of the sFlow system.

Figure 40: sFlow Technology Monitoring System



Configuration

To configure sFlow technology, perform the following tasks:

CLI Quick Configuration

To quickly configure sFlow technology, copy the following commands and paste them into the switch terminal window:

```
[edit protocols]
set sflow collector 10.204.32.46 udp-port 5600

set sflow interfaces ge-0/0/0
set sflow polling-interval 20
set sflow sample-rate egress 1000
```

Step-by-Step Procedure

To configure sFlow technology:

1. Configure the IP address and UDP port of the collector:

```
[edit protocols]
user@switch# set sflow collector 10.204.32.46 udp-port 5600
```

> **NOTE:** You can configure a maximum of 4 collectors.
>
> The default UDP port is 6343.

2. Enable sFlow technology on a specific interface:

```
[edit protocols sflow]
user@switch# set interfaces ge-0/0/0
```

> **NOTE:** You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.
>
> You cannot enable sFlow technology on a link aggregation group (LAG) interface, but you can enable it on the member interfaces of a LAG.

3. Specify in seconds how often the sFlow agent polls the interface:

```
[edit protocols sflow]
user@switch# set polling-interval 20
```

> **NOTE:** The polling interval can be specified as a global parameter also. Specify **0** if you do not want to poll the interface.

4. Specify the rate at which egress packets must be sampled:

```
[edit protocols sflow]
user@switch# set sample-rate egress 1000
```

> **NOTE:** You can specify both egress and ingress sampling rates. If you set only the **egress** sampling rate, the **ingress** sampling rate will be disabled.

> **NOTE:** We recommend that you configure the same sampling rates on all the ports on a line card. If you configure different sampling rates are different, the lowest value is used for all ports. You could still configure different rates on different line cards.

Results

Check the results of the configuration:

```
[edit protocols sflow]
   user@switch# show
polling-interval 20;
   sample-rate egress 1000;
   collector 10.204.32.46 {
      udp-port 5600;
   }
interfaces ge-0/0/0.0;
```

Verification

IN THIS SECTION

- Verifying That sFlow Technology Is Configured Properly | **988**
- Verifying That sFlow Technology Is Enabled on the Specified Interface | **989**
- Verifying the sFlow Collector Configuration | **989**

To confirm that the configuration is correct, perform these tasks:

Verifying That sFlow Technology Is Configured Properly

Purpose

Verify that sFlow technology is configured properly.

Action

Use the **show sflow** command:

```
user@switch> show sflow
```

```
sFlow: Enabled
Sample limit: 300 packets/second
Polling interval: 20 seconds
Sample rate egress: 1:1000: Enabled
Sample rate ingress: 1:2048: Disabled
Agent ID: 10.204.96.222
```

NOTE: The sampling limit cannot be configured and is set to 300 packets/second per FPC.

Meaning

The output shows that sFlow technology is enabled and specifies the values for the sampling limit, polling interval, and the egress sampling rate.

Verifying That sFlow Technology Is Enabled on the Specified Interface

Purpose

Verify that sFlow technology is enabled on the specified interfaces and display the sampling parameters.

Action

Use the **show sflow interface** command:

```
user@switch> show sflow interface
```

```
Interface       Status     Sample rate    Adapted sample rate   Polling-interval

           Egress Ingress   Egress Ingress   Egress Ingress
ge-0/0/0.0 Enabled  Disabled  1000    2048    1000     2048           20
```

Meaning

The output indicates that sFlow technology is enabled on the ge-0/0/0.0 interface with an egress sampling rate of 1000, a disabled ingress sampling rate, and a polling interval of 20 seconds.

Verifying the sFlow Collector Configuration

Purpose

Verify the sFlow collector's configuration.

Action

Use the **show sflow collector** command:

```
user@switch> show sflow collector

Collector          Udp-port    No. of samples
 address
10.204.32.46       5600        1000
10.204.32.76       3400        1000
```

Meaning

The output displays the IP address of the collectors and the UDP ports. It also displays the number of samples.

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch | 982

Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers

IN THIS SECTION

- Requirements | 991
- Overview and Topology | 991
- Configuration | 992
- Verification | 995

sFlow technology is a networking monitoring technology for high-speed switched or routed networks. It is a technology that is based on statistical sampling. You can configure sFlow technology to continuously monitor traffic at wire speed on all interfaces simultaneously. sFlow data can be used to provide network traffic visibility information. You can specify sampling rates for ingress and egress packets. Junos OS fully

supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

This example describes how to configure and use sFlow technology to monitor network traffic.

Requirements

This example uses the following hardware and software components:

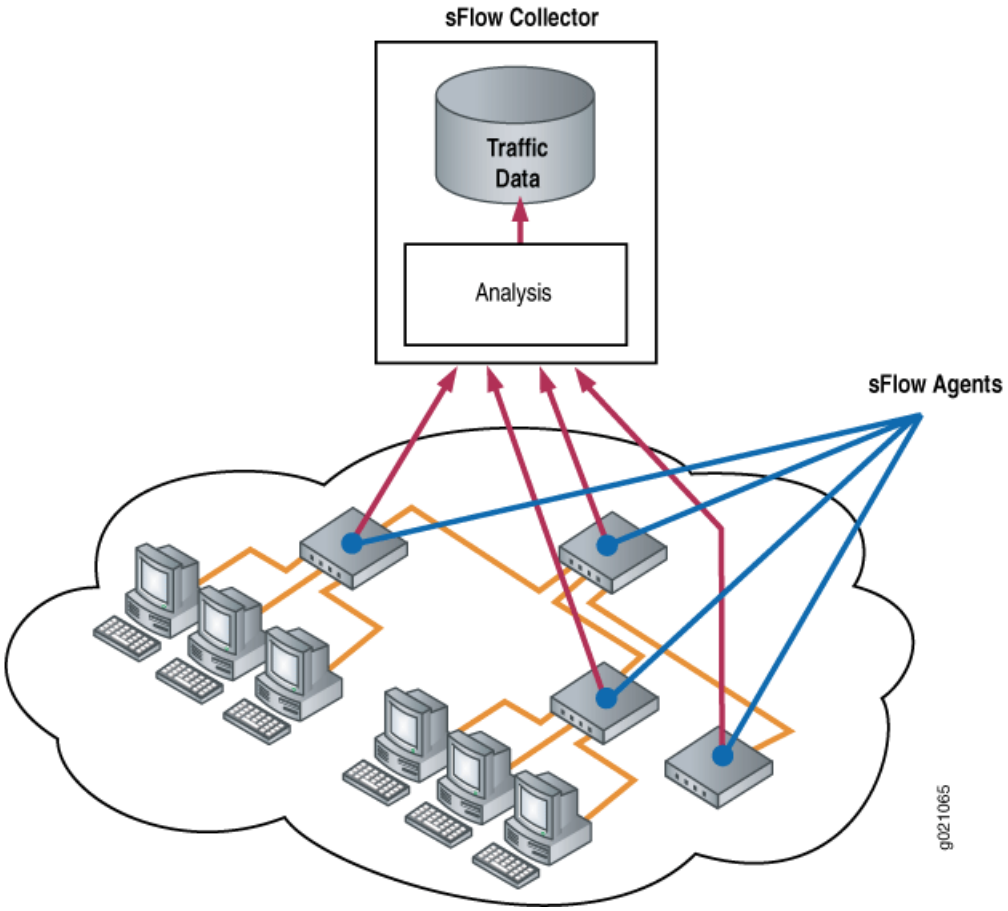
- One MX Series router
- Junos OS Release 18.1 or later for MX Series routers

Overview and Topology

sFlow technology samples network packets and sends the samples to a monitoring station. You can specify sampling rates for ingress and egress packets. The information gathered is used to create a network traffic visibility picture.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent runs on the switch. It combines interface counters and flow samples and sends them across the network to the sFlow collector. Figure 40 on page 986 depicts the basic elements of the sFlow system.

Figure 41: sFlow Technology Monitoring System



Configuration

To configure sFlow technology, perform the following tasks:

CLI Quick Configuration

To quickly configure sFlow technology, copy the following commands and paste them into the router terminal window:

```
[edit protocols]
set sflow collector 10.204.32.46 udp-port 5600

set sflow interfaces ge-0/0/0
set sflow polling-interval 20
set sflow sample-rate egress 1000
set sflow interfaces ge-0/0/1 polling-interval 10 sample-rate ingress 1000
```

Step-by-Step Procedure

To configure sFlow technology:

1. Configure the IP address and UDP port of the collector:

```
[edit protocols]
user@host# set sflow collector 10.204.32.46 udp-port 5600
```

> **NOTE:** You can configure a maximum of 4 collectors.
>
> The default UDP port is 6343.

2. Enable sFlow technology on a specific interface:

```
[edit protocols sflow]
user@host# set interfaces ge-0/0/0
```

> **NOTE:** You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.
>
> You cannot enable sFlow technology on a link aggregation group (LAG) interface, but you can enable it on the member interfaces of a LAG.

3. Specify in seconds how often the sFlow agent polls the interface:

```
[edit protocols sflow]
user@host# set polling-interval 20
```

> **NOTE:** The polling interval can be specified as a global parameter also. Specify **0** if you do not want to poll the interface.

4. Specify the global rate at which egress packets must be sampled:

```
[edit protocols sflow]
user@host# set sample-rate egress 1000
```

> **NOTE:** You can specify both egress and ingress sampling rates. If you set only the **egress** sampling rate, the **ingress** sampling rate will be disabled.

5. Specify the interface level poling rate and sampling rate:

```
[edit protocols sflow]
user@host# set interfaces ge-0/0/1 polling-interval 10 sample-rate ingress 1000
```

> **NOTE:** When you configure at both interface level and global level, former takes the precedence.

> **NOTE:** We recommend that you configure the same sampling rates on all the ports on a line card. If you configure different sampling rates are different, the lowest value is used for all ports. You could still configure different rates on different line cards.

Results

Check the results of the configuration:

```
[edit protocols sflow]
   user@host# show
polling-interval 20;
   sample-rate egress 1000;
   collector 10.204.32.46 {
      udp-port 5600;
   }
   interfaces ge-0/0/0.0;
interfaces ge-0/0/1.0; {
   polling-interval 10;
      sample-rate egress 1000;
   }
```

Verification

IN THIS SECTION

- Verifying That sFlow Technology Is Configured Properly | 995
- Verifying That sFlow Technology Is Enabled on the Specified Interface | 996
- Verifying the sFlow Collector Configuration | 996

To confirm that the configuration is correct, perform these tasks:

Verifying That sFlow Technology Is Configured Properly

Purpose

Verify that sFlow technology is configured properly.

Action

Use the **show sflow** command:

```
user@host> show sflow
```

```
sFlow                    : Enabled
Sample limit             : 300 packets/second
Polling interval         : 20 second
Sample rate egress       : 1:2048: Disabled
Sample rate ingress      : 1:2048: Disabled
Agent ID                 : 10.213.0.18
Agent ID IPv6            : fec0::a:0:0:4
Source IP address        : 10.1.1.1
Source IPv6 address      : fe80::200:ff:fe00:4
```

NOTE: The sampling limit cannot be configured and is set to 300 packets/second per FPC.

Meaning

The output shows that sFlow technology is enabled and specifies the values for the sampling limit, polling interval, and the egress sampling rate.

Verifying That sFlow Technology Is Enabled on the Specified Interface

Purpose

Verify that sFlow technology is enabled on the specified interfaces and display the sampling parameters.

Action

Use the **show sflow interface** command:

```
user@host> show sflow interface
```

```
Interface     Status     Sample rate         Adapted sample rate Polling-interval



               Egress  Ingress    Egress   Ingress      Egress   Ingress
 ge-0/0/0.0    Enabled Disabled   1000     2048         1000     2048       20
 ge-0/0/1.0    Enabled Enabled    1000     1000         1000     1000       10
```

Meaning

The output indicates that sFlow technology is enabled on the ge-0/0/0.0 interface with an egress sampling rate of 1000, a disabled ingress sampling rate, and a polling interval of 20 seconds. Similarly, sFlow is also enabled on the ge-0/0/1.0 interface with an egress sampling rate of 1000, an ingress sampling rate of 1000, and a polling interval of 10 seconds

Verifying the sFlow Collector Configuration

Purpose

Verify the sFlow collector's configuration.

Action

Use the **show sflow collector** command:

```
user@host> show sflow collector
```

```
Collector         Udp-port    No. of samples
 address
10.204.32.46      5600        1000
10.204.32.76      3400        1000
```

Meaning

The output displays the IP address of the collectors and the UDP ports. It also displays the number of samples.

RELATED DOCUMENTATION

Understanding How to Use sFlow Technology for Network Monitoring | 975

Configuring sFlow Technology for Network Monitoring (CLI Procedure)

sFlow technology is a network monitoring technology for high-speed switched or routed networks. It is a technology that is based on statistical sampling. You can configure sFlow technology to continuously monitor traffic at wire speed on all interfaces simultaneously. Junos OS fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

On the QFabric system, the sFlow monitoring global configuration that is defined on the Director device is distributed to Node groups that have sFlow sampling configured on the interfaces.

To configure sFlow features:

1. Configure the IP address and the UDP port of the collector:

   ```
   [edit protocols]
   user@device# set sflow collector ip-address udp-port port-number
   ```

   The default UDP port is 6343,

2. Enable sFlow technology on a specific interface.

   You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement.

   ```
   [edit protocols sflow]
   user@device# set interfaces interface-name
   ```

   Be aware of the following caveats about sFlow on interfaces:

   - With the exception of the QFX10000 Series switches, you cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.
   - You cannot enable sFlow technology on a link aggregation group (LAG), but you can enable it on the member interfaces of a LAG.
   - sFlow technology is not supported on a VXLAN interface.

3. Specify in seconds how often the sFlow agent polls interfaces:

   ```
   [edit protocols sflow]
   user@device# set polling-interval seconds
   ```

> **NOTE:** Specify **0** if you do not want to poll the interface.

4. Specify the rate at which packets must be sampled. You can specify either an egress or an ingress sampling rate, or both.

   > **NOTE:** We recommend that you configure the same sampling rates on all the ports on a line card. If you configure different sampling rates on different ports, the lowest value is used for all ports. You could still configure different rates on different line cards.

   To specify an egress sampling rate:

   ```
   [edit protocols sflow]
   user@device# set sample-rate egress number
   ```

   To specify an ingress sampling rate:

   ```
   [edit protocols sflow]
   user@device# set sample-rate ingress number
   ```

5. (Optional) You can also configure the polling interval and the egress and ingress sampling rates at the interfaces level:

   ```
   [edit protocols sflow interfaces interface-name]
   user@device# set polling-interval seconds

   [edit protocols sflow interfaces]
   user@device# set sample-rate egress number

   [edit protocols sflow interfaces]
   user@device# set sample-rate ingress number
   ```

   > **NOTE:** The interfaces-level configuration overrides the global configuration for the specified interface.

6. Specify an IP address to be used as the agent ID for the sFlow agent:

   ```
   [edit protocols sflow]
   ```

```
user@device# set agent-id ip-address
```

7. Specify the source IP address to be used for sFlow datagrams:

```
[edit protocols sflow]
user@device# set source-ip ip-address
```

8. (Optional) Set the **disable-sw-rate-limiter** configuration statement so that the sampling rate stays within the maximum hardware sampling rate.

```
[edit protocols sflow]
user@device# set disable-sw-rate-limiter
```

Packet-based sampling in sFlow is implemented in the hardware. If traffic levels are unusually high, the hardware generates more samples than it can handle, and the extra samples are dropped, producing inaccurate results. Enabling the **disable-sw-rate-limiter** statement disables the software rate-limiting algorithm and allows the hardware sampling rate to stay within the maximum sampling rate.

RELATED DOCUMENTATION

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch | **982**
- Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**
- Understanding How to Use sFlow Technology for Network Monitoring | **975**
- Overview of sFlow Technology | **970**
- Example: Monitoring Network Traffic Using sFlow Technology | **999**

Example: Monitoring Network Traffic Using sFlow Technology

IN THIS SECTION

- Requirements | **1000**
- Overview | **1000**
- Configuration | **1001**
- Verification | **1003**

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

This example describes how to configure and use sFlow monitoring on a QFX3500 switch in standalone mode.

Requirements

This example uses the following hardware and software components:

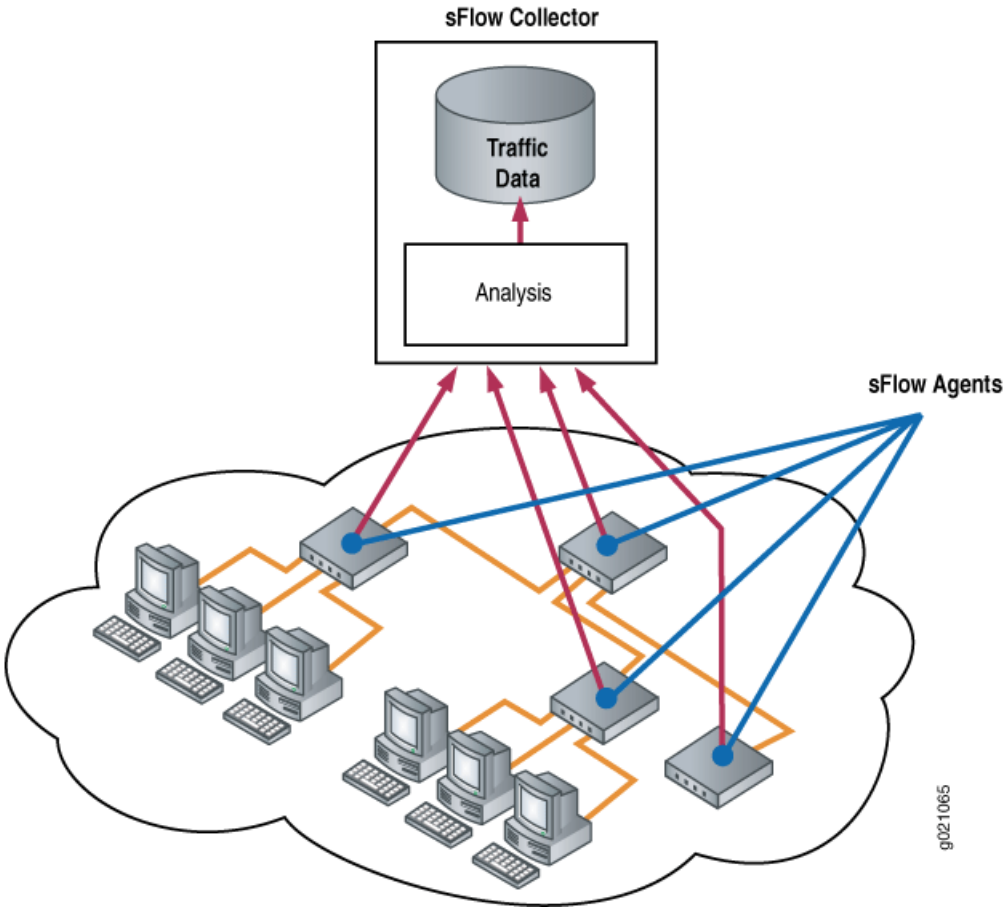
- Junos OS Release 11.3 or later
- One QFX3500 switch

Overview

An sFlow monitoring system consists of an sFlow agent embedded in the device and a centralized collector on the network. The two main activities of the sFlow agent are random sampling and statistics gathering. The sFlow agent combines interface counters and flow samples and sends them to the IP address and UDP destination port of the sFlow collector in UDP datagrams.

Figure 40 on page 986 depicts the basic elements of an sFlow system.

Figure 42: sFlow Technology Monitoring System



Configuration

CLI Quick Configuration

To quickly configure sFlow technology, copy the following commands and paste them into the terminal window of the switch:

```
[edit protocols sflow]
```

set collector 10.204.32.46 udp-port 5600

set interfaces xe-0/0/1.0

set polling-interval 20

set sample-rate 1000

Step-by-Step Procedure

To configure sFlow features using the CLI:

1. Configure the IP address and UDP port of at least one collector:

   ```
   [edit protocols sflow]
   user@switch# set collector 10.204.32.46 udp-port 5600
   ```

   The default UDP port assigned is 6343.

2. Enable sFlow technology on a specific interface:

   ```
   [edit protocols sflow]
   user@switch# set interfaces xe-0/0/1.0
   ```

   > **NOTE:** You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.
   >
   > You cannot enable sFlow technology on a LAG interface (for example, **ae0**), but you can enable sFlow technology on the member interfaces of the LAG (for example, xe-0/0/1).

3. Specify how often (in seconds) the sFlow agent polls all interfaces at the global level:

   ```
   [edit protocols sflow]
   user@switch# set polling-interval 20
   ```

   > **NOTE:** Specify **0** if you do not want to poll the interface.

4. Specify the rate at which packets must be sampled at the global level. The following example sets a sample rate of 1 in 1000 packets:

   ```
   [edit protocols sflow]
   user@switch# set sample-rate 1000
   ```

Results

Check the results of the configuration:

```
[edit]
user@switch# show protocols
sflow {
```

```
    collector 10.204.32.46 {
      udp-port 5600;
    }
    interfaces xe-0/0/1.0 {
      polling-interval 20;
      sample-rate 1000;
    }
  }
```

Verification

IN THIS SECTION

- Verifying That sFlow Technology Has Been Configured Properly | **1003**
- Verifying That sFlow Technology Is Enabled on an Interface | **1004**
- Verifying the sFlow Collector Configuration | **1004**

To confirm that the configuration is correct, perform these tasks:

Verifying That sFlow Technology Has Been Configured Properly

Purpose

Verify that sFlow technology has been configured properly.

Action

Enter the **show sflow** operational mode command:

```
user@switch> show sflow
```

```
sFlow            : Enabled
Sample limit     : 300 packets/second
Polling interval : 20 second
Sample rate      : 1:1000
Agent ID         : 10.1.1.2
```

NOTE: The sample limit cannot be configured and is set to 300 packets per second.

Meaning

The output shows that sFlow technology is enabled and specifies the values for the sampling limit, polling interval, and sampling rate.

Verifying That sFlow Technology Is Enabled on an Interface

Purpose

Verify that sFlow technology is enabled on interfaces and display the sampling parameters.

Action

Enter the **show sflow interface** operational mode command:

```
user@switch> show sflow interface
```

```
Interface       Status     Sample     Polling
                            rate      interval
xe-0/0/1.0   Enabled      1000         20
```

Meaning

The output indicates that sFlow technology is enabled on the **Node1:xe-0/0/1.0** interface on the Node device with a sampling rate of 1000 and a polling interval of 20 seconds.

Verifying the sFlow Collector Configuration

Purpose

Verify the sFlow collector configuration.

Action

Enter the **show sflow collector** operational mode command:

```
user@switch> show sflow collector
```

```
Collector        Udp-port    No. of samples
 address
10.204.32.46         5600           7516
```

Meaning

The output displays the IP address of the collector, the UDP port, and the number of samples collected.

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Overview of sFlow Technology | 970

CHAPTER 28

Packet Flow Accelerator Diagnostics Software

IN THIS CHAPTER

- Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities | **1006**
- Installing Ethernet and PTP Scripts | **1036**
- Installing Packet Flow Accelerator Diagnostics Software | **1038**

Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities

You can use Packet Flow Accelerator Diagnostics software to validate the integrity of the QFX-PFA-4Q module and the QFX5100-24Q-AA switch. The Packet Flow Accelerator Diagnostics software contains standard diagnostics, orchestration diagnostics, Precision Time Protocol (PTP) and synchronization diagnostics, and other utilities. The Packet Flow Accelerator Diagnostics software runs in a guest virtual machine (VM) on the QFX5100-24Q-AA switch and requires that you configure guest VM options in the Junos OS CLI.

The QFX-PFA-4Q module contains four 40-Gigabit Ethernet QSFP+ interfaces, an FPGA module, and timing input and output interfaces to support Precision Time Protocol applications. The FPGA module contains logic that you can customize for processing compute-intensive, latency-sensitive, high-volume transactions.

Before you can run the Packet Flow Accelerator Diagnostics software and utilities, make sure you have performed the following tasks:

- Verify that you have installed the QFX-PFA-4Q module installed on the QFX5100-24Q-AA switch. For more information, see *Installing an Expansion Module in a QFX5100 Device*
- Make sure you have Junos OS Release 14.1X53-D27 with enhanced automation installed on the QFX5100-24Q-AA switch. For more information, see *Installing Software Packages on QFX Series Devices*.

- Install the Packet Flow Accelerator Diagnostics software. For more information, see "Installing Packet Flow Accelerator Diagnostics Software" on page 1038.

- Understanding External and Internal Ports and Network Interface Card Ports | **1007**
- Understanding Packet Flow Accelerator Diagnostics Software Tests and Scripts | **1008**
- Understanding the ikondiag Command | **1009**
- Understanding Basic Functionality Tests | **1010**
- Understanding and Running Ethernet Tests and Scripts | **1012**
- Understanding and Using Stress Tests | **1018**
- Understanding and Running PTP Tests | **1018**
- Understanding QFX-PFA-4Q Module LED Tests | **1020**
- Understanding Packet Flow Accelerator Diagnostics Utilities | **1021**
- Sample Output for Packet Accelerator Diagnostics Software | **1028**

Understanding External and Internal Ports and Network Interface Card Ports

Packet Flow Accelerator Diagnostics software and utilities validate the data paths between the external and internal ports on the QFX5100-24Q-AA switch and QFX-PFA-4Q module. Figure 43 on page 1007 illustrates the names of the ports on the QFX5100-24Q-AA switch and QFX-PFA-4Q module and how they connect.

Figure 43: Ports on the QFX5100-24Q-AA switch and QFX-PFA-4Q module

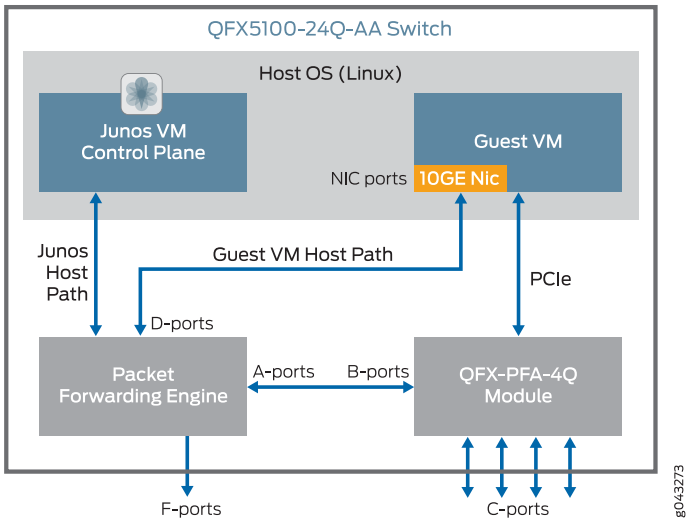


Table 87 on page 1008 provides information on the external and internal ports and NIC ports on the QFX5100-24Q-AA switch and QFX-PFA-4Q module.

Table 87: External and Internal Ports on the QFX5100-24Q-AA Switch and the QFX-PFA-4Q Module

A-ports	Interfaces xe-0/0/24 through xe-0/0/39 on the Packet Forwarding Engine (PFE) of the QFX5100-24Q-AA switch connect to the B-ports on the FPGA module on the QFX-PFA-4Q expansion module. A-ports require corresponding B-ports on the FPGA module. You can manage these interfaces through the Junos OS.
B-ports	Internal 10-Gigabit Ethernet ports connect to the FPGA module on the QFX-PFA-4Q module, which then connect to the A-ports on the PFE of the QFX5100-24Q-AA switch. The naming convention for these ports is determined by the guest VM. The guest VM controls the FPGA module.
C-ports	Four, front-facing 40-Gigabit Ethernet ports on the QFX-PFA-4Q module connect to the FPGA module running on the QFX5100-24Q-AA switch and the F-ports on the QFX5100-24Q-AA switch. The guest VM controls the FPGA module.
D-ports	Two 10-Gigabit Ethernet internal ports on the Packet Forwarding Engine of the QFX5100-24Q-AA switch connect to the Ethernet NIC on the QFX5100-24Q-AA switch. The naming convention for these ports is the same one used for the F-ports. You can manage these ports through the Junos OS.
F-ports	Twenty four front-facing 40-Gigabit Ethernet ports on the QFX5100-24Q-AA switch. These ports contain an “et” prefix when in 40-Gigabit Ethernet mode. If you channelize these interfaces, the prefix is “xe.” You can manage these ports through the Junos OS.
NIC ports	Internal interfaces xe-0/0/40 and xe-0/0/41 on the QFX5100-24Q-AA switch connect to the PFE for use on the guest VM. The NIC ports perform the same functions as any other Linux OS NIC port. The NIC ports do not work unless the QFX-PFA-4Q module is installed.

Understanding Packet Flow Accelerator Diagnostics Software Tests and Scripts

You can run Packet Flow Accelerator Diagnostics software to test the following subsystems on the QFX-PFA-4Q module:

- FPGA
- QDR SRAM memory
- DRAM memory
- DRAM SPDs
- FPGA-connected PCI Express links
- FPGA-connected Ethernet data (QSFP interfaces)

- QSFP I2C I/O
- PTP I/O

Before you can run any test or script, you need to connect to the console connection of the guest VM. For more information, see "Installing Packet Flow Accelerator Diagnostics Software" on page 1038.

The following test sets are available:

- quick-test—Allows you to perform a basic test of all FPGA-attached functionality. These tests take one or two minutes to complete.
- burn-in—Allows you to exercise all FPGA-attached functionality. These tests take several hours to complete.
- individual test mode—Allows you to test a single subsystem with extra configuration options.

Understanding the ikondiag Command

To run any of the tests, issue the **ikondiag** command with the following arguments:

> **NOTE:** Before you can run the tests, you need to connect to the console connection of the guest VM. For more information, see "Installing Packet Flow Accelerator Diagnostics Software" on page 1038.

- -t (quick-test | burn-in | <test name>)

  This argument identifies the test.

- -h

  This argument provides usage details for the test.

- -V

  This argument provides verbose output for the tests.

For example, to run the PTP test, issue the ikondiag -t PTP command at the guest VM prompt:

ikondiag -t PTP

```
[2015-05-07 03:12:20][BEGIN TEST - PTP]


**************************************************************************
```

```
PTP PHY interrupt: PASS

1G Ethernet PHY packet loopback test: PASS

PTP clock generation/check: PASS

UART (ToD) loopback: PASS

**************************************************************************

[2015-05-07 03:13:30][END TEST PTP RESULT PASS]
```

Understanding Basic Functionality Tests

You can test basic functionality on the PCI Express interface and memory components. Table 88 on page 1010 lists the names of the tests and their functions.

Table 88: Base Tests

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior
FPGABasic	Tests basic FPGA operation.	Configures the FPGA and reads some simple registers over PCI Express.	None.	quick-test and burn-in	Any failures in this test cause the **ikondiag** command to generate normal test status and error messages, and then to abort with another error message. You cannot continue testing because all tests rely on the functionality tested by this one.

Table 88: Base Tests *(continued)*

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior
PCIe	Verifies functionality and stability of bulk transfers of PCIe data.	Repeatedly loops back pseudo random data generated on the CPU to the FPGA and then back to the CPU. Returned data is verified on the CPU.	-i <n> number of repetitions (default = 1 quick-test, 10,000 burn-in) -j <n> size of individual transfer in Mebibytes (default = 100 MiB).	quick-test and burn-in	This test reports erroneous data values and offsets in data transfer. Any failures in this test will cause the ikondiag command to output normal test status and error messages and then abort with a further error. You cannot continue further testing because all tests rely on functionality tested by this test.
DIMM	Checks SPD query functionality and verifies that correct DIMMs are installed.	Reads data from SPD device on DIMM modules ,reports contents, and checks for erroneous values and verifies: • DIMM part data against expected part data. • SPD temperature is in nominal operating range.	None.	quick-test and burn-in	If any values are unexpected, the test reports erroneous values and provides expected values and ranges.

Table 88: Base Tests *(continued)*

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior

DRAMMemory	Tests data transfer functionality and stability of FPGA-attached DRAM memory devices.	• Checks that PHYs are initialized correctly.
		• Repeatedly does the following tasks:
		  ◦ Writes to memory from the FPGA
		  ◦ Each pass switches data between: zeros, ones, counter, random, zeros, random, ones, random.
		  ◦ Loops back memory inside the FPGA (simultaneous reads and writes).
		  ◦ Verifies memory from the FPGA
			-i <n> vary number of iterations) default = 1 for quick-test, 500 for burn-in)	quick-test and burn-in	This test reports the number of errors during verification. Number of errors are specified as an accumulated number of errors per byte-lane and DIMM module.

Understanding and Running Ethernet Tests and Scripts

The Ethernet tests and scripts test C-ports and traffic between A- and B-ports. The traffic between A- and B-ports is tested by passing the data on the F-ports. For the C-ports, you need to loop back the traffic sent on the C-ports. You can use physical copper loopback cables for this purpose. For the F-ports, , you need to loop back the traffic sent on the F-ports. You can use copper loopback cables for this purpose. Include the F-ports in a VLAN. You can use the python PFAD_exec.py -t 1 script as well as the tests below. The python PFAD_exec.py -t 1 script verifies end-to-end L2 traffic on the external QSFP ports and checks the statistics on the interfaces in Junos OS and the statistics on the interfaces in the Packet Flow Diagnostics software VM. This test will fail if traffic loss is seen on any of the interfaces. There is also a provision to test all the combinations of QSFP ports as well.

Table 89 on page 1013 lists the names of the Ethernet tests and their functions. For information on how to install the script, see “Installing Packet Flow Accelerator Diagnostics Software” on page 1038.

Table 89: Ethernet Tests and Scripts

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior
QSFPEthernet	Verifies functionality of Ethernet (QSFP) links.	Generates, receives, and verifies Ethernet frames are at line-rate through the FPGA module. The contents and lengths of packets consist of pseudo-random data. During operation, QSFP connections are all channelized to use 10 Gigabit Ethernet with all 32 Ethernet channels operating in parallel in full-duplex mode.	-i <n> varied number of iterations (default = 1,000 for quick-test, 1e9 for burn-in)	quick-test and burn-in	If the number of packets sent or received correctly are verified as not being equal, this test is considered a failure and the discrepancies between these quantities are reported. This test fails if the external Ethernet connections are not configured for loopback.
QSFPI2C	Checks if there is access to the four QSFP modules located on the front of the QFX-PFA-4Q module.	Performs reads of registers in the I2C modules and verifies that the results are as expected. For this test to pass, QSFP media must be inserted into all four ports on the QFX-PFA-4Q module. Any kind of external media can be used (for example, DAC cables, copper loopback, modules, and optical modules).	None.	quick-test and burn-in	This test fails if it cannot detect the presence of a QSFP module or if the values it reads back are unexpected.

Before you can run the Ethernet tests and script successfully, you need to perform the following tasks:

- Externally loop back all of the Ethernet connections (QSFP) on the QFX-PFA-4Q module.

  To loop back the QSFP interfaces on the QFX-PFA-4Q module, attach copper loopback modules on the four QSFP+ interfaces installed on the QFX-PFA-4Q module.

  Attach copper loopback modules on the QSFP+ interfaces (ports 10 through port 13) installed on the QFX5100-24Q-AA switch.
- Channelize ports 10 through 13 on the QFX5100-24Q-AA switch.
- Pair each of the 16 ikonDiag lanes using the equivalent Junos OS interface names with each of the corresponding Junos OS interfaces that were channelized from ports 10 through 13 on the QFX5100-24Q-AA switch.

NOTE: Each VLAN must be independent contain exactly two associated ports—one 10-Gigabit Ethernet port that is an F-port, and one 10-Gigabit Ethernet port that is an A-port.

Table 90 on page 1014 shows the mappings for the 10-Gigabit Ethernet channels on the QFX-PFA-4Q module F-ports.

Table 90: 10-Gigabit Ethernet Channel Mappings on the QFX-PFA-4Q module F-ports

ikondiag Names	Description
JDFE_XE32_10G	xe-0/0/32
JDFE_XE33_10G	xe-0/0/33
JDFE_XE34_10G	xe-0/0/34
JDFE_XE35_10G	xe-0/0/35
JDFE_XE24_10G	xe-0/0/24
JDFE_XE25_10G	xe-0/0/25
JDFE_XE26_10G	xe-0/0/26
JDFE_XE27_10G	xe-0/0/27
JDFE_XE28_10G	xe-0/0/28
JDFE_XE29_10G	xe-0/0/29
JDFE_XE30_10G	xe-0/0/30
JDFE_XE31_10G	xe-0/0/31
JDFE_XE36_10G	xe-0/0/36
JDFE_XE37_10G	xe-0/0/37
JDFE_XE38_10G	xe-0/0/38
JDFE_XE39_10G	xe-0/0/39

Table 91 on page 1015 shows the mappings for the 10-Gigabit Ethernet channels on the QFX-PFA-4Q module C-ports.

Table 91: 10-Gigabit Ethernet Channel Mappings on the QFX-PFA-4Q module C-ports

ikondiag Names	Description
JDFE_QSFP0_10G_PORT0	QSFP port #0 10G sub-channel 0
JDFE_QSFP0_10G_PORT1	QSFP port #0 10G sub-channel 1
JDFE_QSFP0_10G_PORT2	QSFP port #0 10G sub-channel 2
JDFE_QSFP0_10G_PORT3	QSFP port #0 10G sub-channel 3
JDFE_QSFP1_10G_PORT0	QSFP port #1 10G sub-channel 0
JDFE_QSFP1_10G_PORT1	QSFP port #1 10G sub-channel 1
JDFE_QSFP1_10G_PORT2	QSFP port #1 10G sub-channel 2
JDFE_QSFP1_10G_PORT3	QSFP port #1 10G sub-channel 3
JDFE_QSFP2_10G_PORT0	QSFP port #2 10G sub-channel 0
JDFE_QSFP2_10G_PORT1	QSFP port #2 10G sub-channel 1
JDFE_QSFP2_10G_PORT2	QSFP port #2 10G sub-channel 2
JDFE_QSFP2_10G_PORT3	QSFP port #2 10G sub-channel 3
JDFE_QSFP3_10G_PORT0	QSFP port #3 10G sub channel 0
JDFE_QSFP3_10G_PORT1	QSFP port #3 10G sub-channel 1
JDFE_QSFP3_10G_PORT2	QSFP port #3 10G sub-channel 2
JDFE_QSFP3_10G_PORT3	QSFP port #3 10G sub-channel 3

Table 92 on page 1015 provides exact connectivity between the C-ports and A-ports.

Table 92: Exact Connectivity Between C-Ports and A-Ports

QSFP Port Number	Channel Number	Junos OS Interface
QSFP port #0	channel 0	xe-0/0/32

Table 92: Exact Connectivity Between C-Ports and A-Ports *(continued)*

QSFP Port Number	Channel Number	Junos OS Interface
QSFP port #0	channel 1	xe-0/0/33
QSFP port #0	channel 2	xe-0/0/34
QSFP port #0	channel 3	xe-0/0/35
QSFP port #1	channel 0	xe-0/0/24
QSFP port #1	channel 1	xe-0/0/25
QSFP port #1	channel 2	xe-0/0/26
QSFP port #1	channel 3	xe-0/0/27
QSFP port #2	channel 0	xe-0/0/28
QSFP port #2	channel 1	xe-0/0/29
QSFP port #2	channel 2	xe-0/0/30
QSFP port #2	channel 3	xe-0/0/31
QSFP port #3	channel 0	xe-0/0/36
QSFP port #3	channel 1	xe-0/0/37
QSFP port #3	channel 2	xe-0/0/38
QSFP port #3	channel 3	xe-0/0/39

- Add these interfaces to a VLAN.

Channelize ports 10 through 13 using the Junos CLI.

1. Configure ports 10 through 13 on PIC 1 to operate as 10-Gigabit Ethernet ports.

```
[edit chassis fpc 0 pic 1]
user@switch# set port-range 10 13 channel-speed 10g
```

2. Review your configuration and issue the **commit** command.

```
[edit]
user@switch# commit
commit complete
```

Add the 16 channelized interfaces you just configured to 16 VLANs.

To add the 16 channelized interfaces:

1. Create 16 VLANs.

```
[edit vlans]
user@switch# set v0_0 vlan-id 10
user@switch# set v0_1 vlan-id 11
user@switch# set v0_2 vlan-id 12
user@switch# set v0_3 vlan-id 13
user@switch# set v1_0 vlan-id 14
user@switch# set v1_1 vlan-id 15
user@switch# set v1_2 vlan-id 16
user@switch# set v1_3 vlan-id 17
user@switch# set v2_0 vlan-id 18
user@switch# set v2_1 vlan-id 19
user@switch# set v2_2 vlan-id 20
user@switch# set v2_3 vlan-id 21
user@switch# set v3_0 vlan-id 22
user@switch# set v3_1 vlan-id 23
user@switch# set v3_2 vlan-id 24
user@switch# set v3_3 vlan-id 25
```

2. Add the channelized interfaces to the VLANs.

```
[edit interfaces]
user@switch# set xe-0/0/24 unit 0 family ethernet-switching vlan members v0_0
user@switch# set xe-0/0/25 unit 0 family ethernet-switching vlan members v0_1
user@switch# set xe-0/0/10:0 unit 0 family ethernet-switching vlan members v0_0
user@switch# set xe-0/0/10:1 unit 0 family ethernet-switching vlan members v0_1
user@switch# set xe-0/0/10:2 unit 0 family ethernet-switching vlan members v0_2
user@switch# set xe-0/0/10:3 unit 0 family ethernet-switching vlan members v0_3
user@switch# set xe-0/0/11:0 unit 0 family ethernet-switching vlan members v1_0
user@switch# set xe-0/0/11:1 unit 0 family ethernet-switching vlan members v1_1
user@switch# set xe-0/0/11:2 unit 0 family ethernet-switching vlan members v1_2
user@switch# set xe-0/0/11:3 unit 0 family ethernet-switching vlan members v1_3
user@switch# set xe-0/0/12:0 unit 0 family ethernet-switching vlan members v2_0
user@switch# set xe-0/0/12:1 unit 0 family ethernet-switching vlan members v2_1
user@switch# set xe-0/0/12:2 unit 0 family ethernet-switching vlan members v2_2
```

```
user@switch# set xe-0/0/12:3 unit 0 family ethernet-switching vlan members v2_3
user@switch# set xe-0/0/13:0 unit 0 family ethernet-switching vlan members v3_0
user@switch# set xe-0/0/13:1 unit 0 family ethernet-switching vlan members v3_1
user@switch# set xe-0/0/13:2 unit 0 family ethernet-switching vlan members v3_2
user@switch# set xe-0/0/13:3 unit 0 family ethernet-switching vlan members v3_3
```

3. Review your configuration and issue the **commit** command.

```
[edit]
user@switch# commit
commit complete
```

Understanding and Using Stress Tests

The stress tests exercise all high-speed I/Os in parallel. The stress tests require the same external media as you used for the Ethernet tests.Table 93 on page 1018 lists the name of the test and its functions.

Table 93: Stress Tests

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior
Stress	Exercises all high-speed I/Os in parallel.	Exercise all of the high-speed I/Os attached to the FPGA in parallel, including: • DRAM • QDR • Ethernet Each test subsystem is exercised in a similar fashion to the individual tests as previously described.	-i <n> varied number of iterations) default = 1 for quick-test, 1,000 for burn-in)	quick-test and burn-in	If any one sub-system fails, the test is stopped. The first sub-system detected to have failed is reported. **NOTE:** If multiple subsystems fail, only the first failed subsystem is reported.

Understanding and Running PTP Tests

You can run PTP for hardware used with PTP. These tests are helpful if you are creating timing applications. To run the tests, you need to connect SubMiniature version B (SMB) cables, Ethernet loopback cables, and ToD loopback cables for the clocking I/O, ToD serial port, and 1-Gigabit Ethernet connectors. You must connect the SMB, Ethernet, ToD loopback cables between the 10M and PPS output and input

connectors. The ToD loopback cable is a standard RJ45 cable with Pin 3 (Tx Data) connected to Pin 6 (Rx Data). In addition to the PTP tests, you can run scripts included the Packet Flow Accelerator Diagnostics software to test PTP. See Table 95 on page 1020 for information on the PTP scripts. The PTP scripts require you to have a Junos OS image with Enhanced Automation installed on the QFX5100-24Q-AA switch. For information on how to install the scripts, see "Installing Packet Flow Accelerator Diagnostics Software" on page 1038.

Table 94 on page 1019 lists the names of the PTP tests and their functions:

Table 94: PTP Tests

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior

PTP	Checks functionality of various FPGA-attached time-synchronizing features of the QFX-PFA-4Q module.	Performs various tests on time-synchronizing functionality of the QFX-PFA-4Q module.
		
		Subtests covered by this test include:
		
		• Verification of PFE-attached communications.
		• Testing of the PTP PHY
		  ◦ Basic configuration.
		  ◦ FPGA-attached interrupt line.
		  ◦ 1-Gigabit Ethernet loopback (requires external loopback media).
		  ◦ QFX-PFA-4Q module time-syncing related clock generators and feedback routing.
		  ◦ ToD UART port (requires external loop-back media).
			None.	quick-test and burn-in	A failure in any of the subsystems above causes the entire test to fail and generates a report at the end of the test that indicates the pass and fail status of the sub-tests.

Table 95 on page 1020 lists the name of the script and its function. This script is not part of the **ikondiag** command. You can run this command Junos OS.

Table 95: PTP Script

Script Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior

./run_ptp_test	Checks functionality of various FPGA-attached time-syncing features of the QFX-PFA-4Q module.	Performs various tests on time-syncing functionality of the QFX-PFA-4Q module.
		Sub tests covered by this test include:
		• Verification of PFE attached communications.
		• Testing of the PTP PHY
		  ◦ Basic configuration.
		  ◦ FPGA-attached interrupt line.
		  ◦ 1-Gigabith Ethernet loop-back (requires external loop-back media).
		  ◦ QFX-PFA-4Q module time-syncing related clock generators and feedback routing.
		  ◦ ToD UART port (requires external loop-back media).
			None.	None. This test must be run manually.	A failure in any of the subsystems above causes the entire test to fail and generates a report at the end of the test that indicates the pass and fail status of the sub-tests.

Understanding QFX-PFA-4Q Module LED Tests

The LED tests examine the LEDs on the QFX-PFA-4Q module.

To run the LED test, issue the **ikon_led_toggle** command. The test might take a few seconds to start because the FPGA is being configured. When you see the message **Toggling LEDs. Send SIGINT (^C) to exit**, the test begins. To terminate the test, type Ctrl-C. Table 96 on page 1021 lists the name of the test and its function.

Table 96: QFX-PFA-4Q Module LED Test

Test Name	Description	Details	Optional Arguments	Test Sets	Failure Behavior
ikon_led_toggle	Flashes the LEDs on the QFX-PFA-4Q module for visual inspection.	The following LEDs on the QFX-PFA-4Q module will repeatedly cycle through the following patterns: **NOTE:** The AL and ST LEDs are not included in this test. • The sixteen bicolor LEDs for QSFP status cycle through green, orange, and off. • S0 and S1 LEDs cycle through green and off. • Bottom-left RJ-45 PTP status LED cycles through green, orange, and off. • Bottom-right RJ-45 PTP status LED cycles through green and off rapidly. • Alarm LEDs cycle through orange, red, and off.	None.	None. This test must be run manually.	LEDs might not flash.

Understanding Packet Flow Accelerator Diagnostics Utilities

In addition to the Packet Flow Accelerator Diagnostic software tests, there are utilities included in the Packet Flow Accelerator Diagnostics software that you can use to further diagnose issues on the QFX-PFA-4Q module.

> **NOTE:** Before you can run the utilities, you need to connect to the console of the guest VM. For more information on how to access the guest VM, see "Installing Packet Flow Accelerator Diagnostics Software" on page 1038.

Table 97 on page 1022 lists the name of the utility and its function.

Table 97: Utilities

Test Name	Descriptions	Details	Expected Output and Behavior
maxtop	Reports FPGA status.	Displays information about the currently configured status of the FPGA module and whether the module is in operation. Checks to make sure very basic driver and FPGA PCI Express link operations are working correctly. If this utility exits with error(s), it is very unlikely that any further FPGA operations will work.	Output should be similar to that shown below. If this output is not shown, there might be a critical failure in the diagnostic software environment, or the PCI Express link to the FPGA is nonfunctional. **MaxTop Tool 2015.1 Found 1 card(s) running MaxelerOS 2015.1 Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423 Mem: 24GB Load average: 0.00, 0.00, 0.00 DFE %BUSY TEMP MAXFILE PID USER TIME COMMAND 0 0.0% - 2fcf249cc7... - - - -**

Table 97: Utilities *(continued)*

Test Name	Descriptions	Details	Expected Output and Behavior
ikon_snake	Enables snake connectivity between all 10-Gigabit Ethernet channels.	Connects the Rx channel of all 32 x 10-Gigabit Ethernet channels on the FPGA module (QSFP interfaces) to the Tx channel of the respective neighboring connection. This allows all 32 channels to be tested using just a 10-Gigabit Ethernet interface external packet generator, copper loopback modules, and a QSFP <-> 4xSFP breakout cable.	After issuing this test, all Ethernet data will be forwarded after the message **'Snake tool loaded. hit 'enter' to exit.'** is displayed. **NOTE:** During the time before the operating message is printed, the FPGA module might be in the process of being configured, so no data is forwarded. Pressing 'enter' will exit the utility. After the test has finished, packet data continues to be forwarded until another Ethernet utility or test is run.

Table 97: Utilities *(continued)*

Test Name	Descriptions	Details	Expected Output and Behavior
ikon_eth_util all --digitalloopback	Enables digital-loopback on all 10-Gigabit Ethernet interfaces on the Enables 'snake' connectivity between all QFX-PFA-4Q module 10-Gigabit Ethernet channels.	Connects the Rx side of all 32x 10-Gigabit Ethernet channels on the FPGA module (QSFP) to the Tx side of the same channel.	After issuing this test, all Ethernet data will be forwarded as described after the message **'running press return key to exit'** is displayed. **NOTE:** Before the operating message is displayed, the FPGA module might be in the process of being configured, and no data will be forwarded. Pressing Enter exits the utility. After the test has finished, packet data continues to be forwarded until another Ethernet utility or test is run.

Table 97: Utilities *(continued)*

Test Name	Descriptions	Details	Expected Output and Behavior
ikon_eth_util	Enables data to pas -through QFX-PFA-4Q module QSFP ports.	Allows data to pass through the QFX-PFA-4Q module QSFP ports on the QFX-PFA-4Q module. **NOTE:** Because all of the QSFP ports are channelized to 10-Gigabit Ethernet, you must use SFP breakout cables when connecting external media.	After issuing this test, all Ethernet data is forwarded as described after the message ‘ running press return key to exit ’ is displayed. **NOTE:** Before the operating message is displayed, the the FPGA module might be in the process of being configured, and no data will be forwarded. Pressing ‘enter’ will exit the utility. After the test has finished, packet data will continue to be forwarded until another Ethernet utility or test is run.

Table 97: Utilities *(continued)*

Test Name	Descriptions	Details	Expected Output and Behavior

maxnet -v link show	Dumps FPGA packet statistics.	Displays statistics about packets sent and received on all (QSFP) links from the MAC and PHY IP cores in the FPGA. Using the 'v' option provides verbose output.
		
		Here are some important items to note:
		
		• Packet statistics are reset whenever the Altera FPGA is reconfigured; that is, when running different applications that make use of the FPGA.
		• The tool only displays data for Ethernet links that are included in the FPGA design. As such, If the FPGA module has not yet been configured, or it is configured with an application that does not use some of the Ethernet links, reduced link details might be displayed.
			Sample output for a single 10-Gigabit Ethernet link is as follows:
			
			`MaxTop Tool 2015.1`
			`Found 1 card(s) running MaxelerOS 2015.1`
			`Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423`
			`Mem: 24GB`
			
			`Load average: 0.00, 0.00, 0.00`
			
			`DFE %BUSY TEMP MAXFILE PID USER TIME COMMAND`
			`0 0.0% - 2fcf249cc7... - - - -`

Table 97: Utilities *(continued)*

Test Name	Descriptions	Details	Expected Output and Behavior
host2mem I <filename> -o <filename> -t <DDR | QDR0 | QDRPARITY0 | QDR1 | QDRPARITY1>	Writes and then reads arbitrary data from QDR SRAM or DRAM.	Operates by streaming the contents of a binary file to one of the memory resources on the QFX-PFA-4Q module through the FPGA, and then streams the same data back from the memory to another file. **NOTE:** You cannot only read back data from RAM because the contents are not preserved between running multiple tests.	Reports PASSED or FAILED depending on whether the returned data matches the input data.

Table 98 on page 1027 lists the command-line arguments for the host2mem utility.

Table 98: Command-Line Arguments

Argument	Description
-- help | -h	Print out usage and exit.
-i <input file>	Input data file.
-o <output file>	Output data file.
-- test | -t <test name>	Test resource. See Table 99 on page 1028 for information regarding resources.
-- verbose | -v	Enable verbose mode.

The file format for input and output files is identical. Data is packed consecutively as words based on the width specified in the test mode table below. The size of an input file might be less but must not exceed the total size of the resource being tested. The size of the output file is the same as the input file and, provided there are no errors, has the same content.

Table 99: File Format Details

Test Mode	Resource	Word Width	Size of Test Data
DDR	DDR SDRAM	192 B	24 GB
QDR0	QDR0 Data	16 B	32 MB
QDRPARITY0	QDR0 Parity bits	2 B	4 MB
QDR1	QDR1 Data	16 B	32 MB
QDRPARITY1	QDR1 Parity bits	2 B	4 MB

The dynamic random-access memory (DRAM) on the QFX-PFA-4Q module contains three dual in-line memory modules (DIMM3, DIMM4, DIMM6), and each data word is split across all three DIMMs.Table 100 on page 1028 lists the allocation of Bytes to DIMMs.

Table 100: Dual In-Line Memory Modules

0	DIMM3	63	64	DIMM4	127	128	DIMM6	191

Sample Output for Packet Accelerator Diagnostics Software

This section provides some sample output for base tests, Ethernet tests, PTP tests, and utilities.

- ikondiag -t FPGABasic

```
[2015-05-07 03:00:17][BEGIN TEST - FPGABasic]
[2015-05-07 03:00:17][END TEST FPGABasic RESULT PASSED]
```

- ikondiag -t DIMM

```
[2015-05-07 03:01:09][BEGIN TEST - DIMM]
[2015-05-07 03:01:09][END TEST DIMM RESULT PASSED]
```

- ikondiag -t QSFPEthernet

```
[2015-05-07 03:02:33][BEGIN TEST - QSFPEthernet]
```

```
**********************************************


Test Failed:


  QSFP0_10G_PORT0: FAIL - packets received = 0/1000


  QSFP0_10G_PORT1: FAIL - packets received = 0/1000


  QSFP0_10G_PORT2: FAIL - packets received = 0/1000


  QSFP0_10G_PORT3: FAIL - packets received = 0/1000
  QSFP1_10G_PORT0: FAIL - packets received = 0/1000


  QSFP1_10G_PORT1: FAIL - packets received = 0/1000


  QSFP1_10G_PORT2: FAIL - packets received = 0/1000


  QSFP1_10G_PORT3: FAIL - packets received = 0/1000


  QSFP2_10G_PORT0: FAIL - packets received = 0/1000


  QSFP2_10G_PORT1: FAIL - packets received = 0/1000


  QSFP2_10G_PORT2: FAIL - packets received = 0/1000


  QSFP2_10G_PORT3: FAIL - packets received = 0/1000


  QSFP3_10G_PORT0: FAIL - packets received = 0/1000
  QSFP3_10G_PORT1: FAIL - packets received = 0/1000
```

```
QSFP3_10G_PORT2: FAIL - packets received = 0/1000

QSFP3_10G_PORT3: FAIL - packets received = 0/1000

QSFP4_10G_PORT0: PASS - packets received = 1000/1000

QSFP4_10G_PORT1: PASS - packets received = 1000/1000

QSFP4_10G_PORT2: PASS - packets received = 1000/1000

QSFP4_10G_PORT3: PASS - packets received = 1000/1000

QSFP5_10G_PORT0: PASS - packets received = 1000/1000

QSFP5_10G_PORT1: PASS - packets received = 1000/1000

QSFP5_10G_PORT2: PASS - packets received = 1000/1000

QSFP5_10G_PORT3: PASS - packets received = 1000/1000

QSFP6_10G_PORT0: PASS - packets received = 1000/1000

QSFP6_10G_PORT1: PASS - packets received = 1000/1000

QSFP6_10G_PORT2: PASS - packets received = 1000/1000

QSFP6_10G_PORT3: PASS - packets received = 1000/1000

QSFP7_10G_PORT0: PASS - packets received = 1000/1000
```

```
  QSFP7_10G_PORT1: PASS - packets received = 1000/1000

  QSFP7_10G_PORT2: PASS - packets received = 1000/1000

  QSFP7_10G_PORT3: PASS - packets received = 1000/1000

*********************************************

[2015-05-07 03:02:41][END TEST QSFPEthernet RESULT PASSED]
```

- ikondiag -t DRAMMemory -i 3

```
[2015-05-07 03:03:37][BEGIN TEST - DRAMMemory]

[2015-05-07 03:04:21][END TEST DRAMMemory RESULT PASSED]
```

- ikondiag -t QDRMemory -p -i 3

```
[2015-05-07 03:10:38][BEGIN TEST - QDRMemory]

[2015-05-07 03:10:45][END TEST QDRMemory RESULT PASSED]
```

- ikondiag -t Stress -p -i 10

```
[2015-05-07 03:11:24][BEGIN TEST - Stress]

*********************************************
```

```
Test Failed:

  QSFP0_10G_PORT0: PASS - packets received = 650000/650000

  QSFP0_10G_PORT1: PASS - packets received = 650000/650000

  QSFP0_10G_PORT2: PASS - packets received = 650000/650000

  QSFP0_10G_PORT3: PASS - packets received = 650000/650000

  QSFP1_10G_PORT0: PASS - packets received = 650000/650000

  QSFP1_10G_PORT1: PASS - packets received = 650000/650000

  QSFP1_10G_PORT2: PASS - packets received = 650000/650000

  QSFP1_10G_PORT3: PASS - packets received = 650000/650000

  QSFP2_10G_PORT0: PASS - packets received = 650000/650000
  QSFP2_10G_PORT1: PASS - packets received = 650000/650000
  QSFP2_10G_PORT2: PASS - packets received = 650000/650000

  QSFP2_10G_PORT3: PASS - packets received = 650000/650000

  QSFP3_10G_PORT0: PASS - packets received = 650000/650000

  QSFP3_10G_PORT1: PASS - packets received = 650000/650000

  QSFP3_10G_PORT2: PASS - packets received = 650000/650000
```

```
QSFP3_10G_PORT3: PASS - packets received = 650000/650000

QSFP4_10G_PORT0: PASS - packets received = 650000/650000

QSFP4_10G_PORT1: PASS - packets received = 650000/650000

QSFP4_10G_PORT2: PASS - packets received = 650000/650000
QSFP4_10G_PORT3: PASS - packets received = 650000/650000

QSFP5_10G_PORT0: PASS - packets received = 650000/650000

QSFP5_10G_PORT1: PASS - packets received = 650000/650000

QSFP5_10G_PORT2: PASS - packets received = 650000/650000

QSFP5_10G_PORT3: PASS - packets received = 650000/650000

QSFP6_10G_PORT0: PASS - packets received = 650000/650000

QSFP6_10G_PORT1: PASS - packets received = 650000/650000
QSFP6_10G_PORT2: PASS - packets received = 650000/650000

QSFP6_10G_PORT3: PASS - packets received = 650000/650000

QSFP7_10G_PORT0: PASS - packets received = 650000/650000

QSFP7_10G_PORT1: PASS - packets received = 650000/650000

QSFP7_10G_PORT2: PASS - packets received = 650000/650000
```

```
  QSFP7_10G_PORT3: PASS - packets received = 650000/650000

*********************************************
```

- ikondiag -t PTP

```
[2015-05-07 03:12:20][BEGIN TEST - PTP]

*************************************************************************

PTP PHY interrupt: PASS

1G Ethernet PHY packet loopback test: PASS

PTP clock generation/check: PASS

UART (ToD) loopback: PASS

*************************************************************************

[2015-05-07 03:13:30][END TEST PTP RESULT PASS]
```

- ikondiag -t Application -i 2

```
iterations = 2
```

```
[2015-05-07 03:14:11][BEGIN TEST - Application Test]


[2015-05-07 03:17:33][END TEST Application Test RESULT PASSED]
```

- maxtop

```
MaxTop Tool 2015.1
Found 1 card(s) running MaxelerOS 2015.1
Card 0: (P/N: 241124) S/N: 96362301684266423 Mem: 24GB

Load average: 0.00, 0.00, 0.00

DFE  %BUSY  TEMP   MAXFILE        PID    USER       TIME      COMMAND
 0   0.0%   -      7e2198e5c0...  -      -          -         -
```

- ikon_eth_util --all-pass-through

```
Ikon Ethernet Pass Through Utility
setting portConnect_QSFP4_10G_PORT0_QSFP0_10G_PORT0 to 1
setting portConnect_QSFP4_10G_PORT1_QSFP0_10G_PORT1 to 1
setting portConnect_QSFP4_10G_PORT2_QSFP0_10G_PORT2 to 1
setting portConnect_QSFP4_10G_PORT3_QSFP0_10G_PORT3 to 1
setting portConnect_QSFP1_10G_PORT0_QSFP5_10G_PORT0 to 1
setting portConnect_QSFP1_10G_PORT1_QSFP5_10G_PORT1 to 1
setting portConnect_QSFP1_10G_PORT2_QSFP5_10G_PORT2 to 1
setting portConnect_QSFP1_10G_PORT3_QSFP5_10G_PORT3 to 1
setting portConnect_QSFP2_10G_PORT0_QSFP6_10G_PORT0 to 1
setting portConnect_QSFP2_10G_PORT1_QSFP6_10G_PORT1 to 1
setting portConnect_QSFP2_10G_PORT2_QSFP6_10G_PORT2 to 1
setting portConnect_QSFP2_10G_PORT3_QSFP6_10G_PORT3 to 1
setting portConnect_QSFP3_10G_PORT0_QSFP7_10G_PORT0 to 1
setting portConnect_QSFP3_10G_PORT1_QSFP7_10G_PORT1 to 1
setting portConnect_QSFP3_10G_PORT2_QSFP7_10G_PORT2 to 1
setting portConnect_QSFP3_10G_PORT3_QSFP7_10G_PORT3 to 1
running press return key to exit
```

RELATED DOCUMENTATION

Installing Packet Flow Accelerator Diagnostics Software | 1038
Installing Ethernet and PTP Scripts | 1036
Installing an Expansion Module in a QFX5100 Device

Installing Ethernet and PTP Scripts

Installing Ethernet and PTP Scripts

You can use Ethernet and PTP scripts that are included in the Packet Flow Accelerator Diagnostics software to test Ethernet and PTP functionality. Before you can install the scripts, you need to perform the following tasks:

- Make sure the QFX-PFA-4Q module is installed in the QFX5100 switch. See *Installing an Expansion Module in a QFX5100 Device* .
- Install Junos OS Release 14.1X53-D27 software or later with enhanced automation for the QFX5100 switch. See *Installing Software Packages on QFX Series Devices* .
- Enable SSH and Telnet services on the switch. See *Configuring SSH Service for Remote Access to the Router or Switch* and *Configuring Telnet Service for Remote Access to a Switch* .
- Install the Packet Flow Accelerator Diagnostics Software. See "Installing Packet Flow Accelerator Diagnostics Software" on page 1038 .

To install the scripts:

1. Log into the guest VM using the **request app-engine virtual-machine-shell *guest-VM-name***. The maximum length for the guest VM name is 255 characters. Make sure you are logged in as root when you enter this command.

   ```
   root> request app-engine virtual-machine-shell diagnostics
   ```

2. Enter a valid username and password combination for the guest VM.

3. Enter the **guest-util diag-install *guest VM IP address*** command at the shell prompt.

   Use the same IP address you used for configuring the local management address for the guest VM.

   ```
   [root@localhost ~] guest-util diag-install 192.168.1.10
   ```

4. Change directories to /var/tmp to edit the PFAD_params.cfg file.

   ```
   [root@localhost ~] cd /var/tmp
   ```

5. Open the PFAD_params.cfg file using an editor of your choice.

Here is an example of what is contained in the file:

```
[params]


# log level
LOGLEVEL = 'TRACE'


# my variables
VLAN1_NAME      = 'VLAN100'
VLAN1_ID        = '100'
JUNOS_USERNAME  = 'test'
ROOT_USERNAME   = 'root'
JUNOS_PSWD      = 'juniper123'
GUEST_PSWD      = 'diag'
ROOT_PSWD       = 'root123'



# my duts
DUTS = {
    'R0': "10.204.43.170",
    }



TOPOLOGY = 'IF1 = 'et-0/0/2’
                                IF2 = ‘et-0/0/3’

PFAD_params.cfg: unmodified: line 1
```

6. Configure the management IP address.

```
                                DUTS = {
                                               ‘R0': "10.204.43.170”,
                                                         }
```

7. Configure the PTP interfaces.

   IF1 is the primary source, and IF2 is the secondary source.

   Configure IF1 as et-0/0/2, and IF2 as et-0/0/3.

```
IF1 = '2'  <<<<< Change it
IF2 = '3'  <<<<< Change it
```

8. Save the changes you made to the PFAD_params.cfg file.

9. Run the scripts by issuing one of the following commands at the guest VM prompt.

   - To test traffic orchestration:

     python PFAD_exec.py -t 1

   - To test PTP:

     ./run_ptp_test

   - To test Broadsync:

     ./run_broadsync_test

RELATED DOCUMENTATION

Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities | 1006

Installing an Expansion Module in a QFX5100 Device

Installing Packet Flow Accelerator Diagnostics Software | 1038

Launching a Guest Virtual Machine (VM) to Run a Third Party Application on Junos OS Release 13.2X51-D20 and Later

Installing Software Packages on QFX Series Devices

Installing Packet Flow Accelerator Diagnostics Software

Installing Packet Flow Accelerator Diagnostics Software

You can use Packet Flow Accelerator Diagnostics software to test the FPGA module in the QFX-PFA-4Q module installed on the QFX5100-24Q-AA switch as well as the data paths between the FPGA module and the QFX5100-24Q-AA switch. The Packet Flow Accelerator Diagnostics software contains standard diagnostics, orchestration diagnostics, and Precision Time Protocol (PTP) and synchronization diagnostics. See “Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities” on page 1006. In addition to the Packet Flow Accelerator Diagnostics software tests, there are utilities included in the Packet Flow Accelerator Diagnostics software that you can use to further diagnose issues on the QFX-PFA-4Q module. For information on how to install the QFX-PFA-4Q module, see *Installing an Expansion Module in a QFX5100 Device*.

To run the orchestration diagnostics, PTP and synchronization diagnostics, and utilities contained in the Packet Flow Accelerator Diagnostics software, you need to have a Junos OS Release 14.1X53-D27 software or later with enhanced automation installed on your QFX5100 switch. For information on how to download and install Junos OS software, see *Installing Software Packages on QFX Series Devices*.

The Packet Flow Accelerator Diagnostics software runs in a guest VM on the switch and requires that you configure guest VM options in the Junos OS CLI.

Verifying That the QFX-PFA-4Q Expansion Module Is Installed

Before you install the Packet Flow Accelerator Diagnostics software, verify that the QFX-PFA-4Q module is installed.

From the CLI prompt, issue the **show chassis hardware** command.

```
{master:0}
```

```
root> show chassis hardware
```

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                VX3715020024      QFX5100-24Q-AA
Pseudo CB 0
Routing Engine 0          BUILTIN      BUILTIN           QFX Routing Engine
FPC 0            REV 02   650-057155   VX3715020024      QFX5100-24Q-AA
  CPU                     BUILTIN      BUILTIN           FPC CPU
  PIC 0                   BUILTIN      BUILTIN           24x 40G-QSFP-AA
    Xcvr 6       REV 01   740-032986   QD334902          QSFP+-40G-SR4
  PIC 1          REV 01   711-060247   VY3115060052      QFX-PFA-4Q
Power Supply 0   REV 03   740-041741   1GA24082731       JPSU-650W-AC-AFO
Power Supply 1   REV 03   740-041741   1GA24082726       JPSU-650W-AC-AFO
Fan Tray 0                                              QFX5100 Fan Tray 0, Front
 to Back Airflow - AFO
Fan Tray 1                                              QFX5100 Fan Tray 1, Front
 to Back Airflow - AFO
Fan Tray 2                                              QFX5100 Fan Tray 2, Front
 to Back Airflow - AFO
Fan Tray 3                                              QFX5100 Fan Tray 3, Front
 to Back Airflow - AFO
Fan Tray 4                                              QFX5100 Fan Tray 4, Front
 to Back Airflow - AFO
```

From the CLI output, you can see that the four QSFP+ interfaces (4x40G QSFP+) contained in the QFX-PFA-4Q module. are installed.

Downloading the Packet Flow Diagnostics Software

> **NOTE:** To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

To download the Packet Flow Diagnostics software package from the Juniper Networks Support website, go to https://www.juniper.net/support/ :

1. Using a Web browser, navigate to https://www.juniper.net/support .
2. Click **Download Software**.
3. In the Switching box, click **Junos OS Platforms**.
4. In the QFX Series section, click the name of the platform for which you want to download software.
5. Click the Software tab and select the release number from the Release drop-down list.
6. In the Install Package section on the Software tab, select the Install Package for the release.

   A login screen appears.
7. Enter your name and password and press Enter.
8. Read the End User License Agreement, click the **I agree** radio button, and then click **Proceed**.
9. Save the **pfadiag_vm-rXXXXX.img.gz** file on your computer.
10. Open or save the Packet Flow Diagnostics software package either to the local system in the **var/tmp** directory or to a remote location. If you are saving the installation package to a remote system, make sure that you can access it using HTTP, TFTP, FTP, or scp.

Copying the Packet Flow Diagnostics Software Package to the Switch

To copy the packet flow diagnostics software package to the switch:

1. Copy the packet flow diagnostics package to the switch using any file transfer protocol:

   For example:

   ```
   root% scp //hostname/pathname/pfadiag_vm-rXXXXX.img.gz /var/tmp
   ```

Install the Packet Flow Diagnostics Software on the Switch

To install the packet flow diagnostics software package on the switch:

1. Install the Packet Flow Diagnostics software on the switch.

   This might take a few minutes.

   If the Packet Flow Diagnostics software resides locally on the switch, issue the following command:

   ```
   {master:0}
   root> request system software add virtual-machine-package /var/tmp/pfadiag_vm-rXXXXX.img.gz
   Installing virtual-machine package..
   Copying virtual-machine package..
   Uncompressing virtual-machine package..
   Finished virtual-machine package installation.
   ```

2. Issue the **show version** command to verify that the installation was successful.

   ```
   {master:0}
   root> show version
   fpc0:


   --------------------------------------------------------------------------


   Hostname: switch


   Model: qfx5100-24q-aa


   Junos: 14.1X53-D27_vjunos.62
   ```

```
JUNOS Base OS Software Suite [14.1X53-D26_vjunos.62]

JUNOS Base OS boot [14.1X53-D27_vjunos.62]

JUNOS Crypto Software Suite [14.1X53-D27_vjunos.62]

JUNOS Online Documentation [14.1X53-D27_vjunos.62]

JUNOS Kernel Software Suite [14.1X53-D27_vjunos.62]

JUNOS Packet Forwarding Engine Support (qfx-ex-x86-32) [14.1X53-D27_vjunos.62]

JUNOS Routing Software Suite [14.1X53-D27_vjunos.62]

JUNOS Enterprise Software Suite [14.1X53-D27_vjunos.62]

JUNOS py-base-i386 [14.1X53-D27_vjunos.62]

JUNOS py-extensions-i386 [14.1X53-D27_vjunos.62]

JUNOS Host Software [14.1X53-D27_vjunos.62]

Junos for Automation Enhancement

JUNOS GUEST-VM Software [pfadiag_vm-rXXXXX-ve]
```

```
{master:0}
```

The CLI output shows that the Packet Flow Accelerator Diagnostics software was installed.

Configure the Guest VM Options to Launch the Guest VM on the Host

To configure the guest VM options:

1. Configure the following options for guest VM support in the Junos OS CLI at the [edit] hierarchy.
   - Compute cluster name
   - Compute node name
   - VM instance name
   - Dedicated management interface for guest VM
   - Third-party package name
   - Internal IP address of the guest VM
2. Configure the name of the compute cluster and compute node.

   The name of the compute cluster must be default-cluster, and the name of the name of the compute node must be default-node; otherwise, launching the guest VM fails.

   ```
   {master:0}
   root# set services app-engine compute-cluster default-cluster compute-node default-node hypervisor
   ```

3. Configure the name of the VM instance and the name of the third party application.

   ```
   {master:0}
   root# set services app-engine virtual-machines instance instance-name package package-name
   ```

   > **NOTE:** The package names in the **show app-engine virtual-machine-package** command and the **show version** command should match.

   ```
   {master:0}
   root# set services app-engine virtual-machines instance diagnostics package pfadiag_vm-rXXXXX-ve
   ```

4. Associate the VM instance with the configured compute cluster and compute node.

   ```
   {master:0}
   ```

```
root# set services app-engine virtual-machines instance instance-name compute-cluster name
compute-node name
```

```
{master:0}
root# set services app-engine virtual-machines instance diagnostics compute-cluster default-cluster
compute-node default-node
```

> **NOTE:** The name of the compute cluster must be default-cluster, and the name of the compute node must be default-node; otherwise, launching the guest VM fails.

5. Configure the local management IP address.

   This IP address is used for the internal bridging interface. The host uses this IP address to check the availability of the guest VM.

   > **NOTE:** Do not use 192.168.1.1 and 192.168.1.2 as IP addresses because they are used by the Host-OS and Junos OS respectively.

   ```
   {master:0}
   root# set services app-engine virtual-machines instance instance-name local-management family
   inet address 192.168.1.X
   ```

   ```
   {master:0}
   root# set services app-engine virtual-machines instance diagnostics local-management family inet
   address 192.168.1.10
   ```

6. Configure the management interface for the guest VM.

   This management interface is separate from the one used for Junos OS.

   ```
   {master:0}
   root # set services app-engine virtual-machines instance diagnostics management-interface em1
   ```

   > **NOTE:** The management interface name must be either em0 or em1. The configuration will fail if you do not configure a management interface and then commit the configuration.

   The new management interface is provisioned for the guest VM.

7. Commit the configuration.

```
{master:0}
root# commit
```

Here are the results of the configuration:

```
services {
    app-engine {
        compute-cluster default-cluster {
            compute-node default-node {
                hypervisor;
            }
        }
        virtual-machines {
            instance diagnostics {
                package pfadiag_vm-rXXXXX-ve;
                local-management {
                    family inet {
                        address 192.168.1.10;
                    }
                }
                compute-cluster default-cluster {
                    compute-node default-node;
                }
                management-interface em1;
            }
        }
    }
}
```

Verifying That the Guest VM is Working

To verify that the guest VM is working:

1. Issue the following **show** commands to verify that everything is working correctly:

   - root> **show app-engine status**

     ```
     Compute cluster: default-cluster
       Compute Node: default-node, Online
     ```

     The status should be Online.

   - root> **show app-engine virtual-machine instance**

     ```
     VM name                  Compute cluster           VM status
     diagnostics               default-cluster           ACTIVE
     ```

     The VM status should be active.

   - root> **show app-engine virtual-machine package**

     ```
     VM package: pfadiag_vm-rXXXXX-ve
     Compute cluster                   Package download status
     default-cluster                   DOWNLOADED
     ```

Accessing the Guest VM

To access the guest VM:

1. Log into the guest VM.

   - Specify the guest VM name using the **request app-engine virtual-machine-shell *guest-VM-name*** command. The maximum length for the guest VM name is 255 characters. Make sure you are logged in as root when you enter this command.

     root> **request app-engine virtual-machine-shell diagnostics**

   - Enter a valid username and password combination for the guest VM.

NOTE: The first time you log in, the username is root. There is no password. After you log in, you will be prompted to create a password.

For example:

```
Maxeler Ikon Diagnostics VM r44702

diagnostics login: root
You are required to change your password immediately (root enforced)
New password:
Retype new password:
```

2. Issue the **ifconfig -a** command to see the names of the management interface that is used to access the guest VM from outside of the network, name of the management interface that is used for internal use, and the NIC ports used in the diagnostics VM.

   In this example, the **heartbeat** address is the IP address that is used for internal use , the **management** interface is used for external communications, and the xe-0/0/40 and xe-0/0/41 interfaces are the NIC ports used in the diagnostics VM. The **heartbeat** is configured by default. The IP address of the **heartbeat** is the same as the IP address you configured for Junos OS.

   You can associate one of the interfaces to the guest VM by issuing the **set services app-engine virtual-machines instance *name* management-interface *interface-name***. command. Use the same IP address as the one you configured using the **set services app-engine virtual-machines instance test local-management family inet address 192.168.1.10**. The MAC addresses associated with these interfaces are used for internal bridging.

   `[root@ikondiag ~]#` **ifconfig -a**

```
heartbeat Link encap:Ethernet  HWaddr 52:54:00:5D:DB:01
          inet addr:192.168.1.10  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe5d:db01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24955 (24.3 KiB)  TX bytes:24232 (23.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

management Link encap:Ethernet  HWaddr 52:54:00:76:B3:C4
          inet6 addr: fe80::5054:ff:fe76:b3c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:438 (438.0 b)  TX bytes:1836 (1.7 KiB)

xe-0-0-40 Link encap:Ethernet  HWaddr EA:8B:BB:75:56:FE
          inet6 addr: fe80::e88b:bbff:fe75:56fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:140 (140.0 b)

xe-0-0-41 Link encap:Ethernet  HWaddr 3E:1A:00:94:ED:5B
          inet6 addr: fe80::3c1a:ff:fe94:ed5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:230 (230.0 b)
```

Verifying That the FPGA Module Is Working

You can use the following utilities to verify that the FPGA module on the QFX-PFA-4Q module is working.

To verify that the FPGA module is working:

1. Issue the **lspci |grep "RAM memory"** command at the guest VM login prompt.

   `[root@ikondiag ~]#` **lspci |grep "RAM memory"**

   ```
   00:09.0 RAM memory: Juniper Networks Device 0078
   ```

   The output shows that Juniper Networks Device 0078 is working.

2. Issue the **lspci |grep Co-processor** command at the guest VM login prompt:

```
[root@ikondiag ~]# lspci |grep Co-processor
:0a.0 Co-processor: Maxeler Technologies Ltd. Device 0006
```

The output shows that Maxeler Technologies Ltd. Device 0006 is working.

3. Issue the **maxtop** command at the guest VM login prompt:

> **NOTE:** If there are errors in the command output, relaunch the guest VM.

```
[root@ikondiag ~]# maxtop
MaxTop Tool 2015.1
Found 1 card(s) running MaxelerOS 2015.1
Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423 Mem: 24GB

Load average: 0.00, 0.00, 0.00

DFE  %BUSY  TEMP   MAXFILE        PID    USER       TIME      COMMAND
 0   0.0%   -      2fcf249cc7...  -      -          -         -
```

Validating Connections Between QFX5100-24Q-AA Switch Network Ports and QFX-PFA-4Q Module Ports

You can use the **ikon_eth_util –all-pass-through** utility to validate the connections between the QFX5100-24Q-AA switch network ports and the QFX-PFA-4Q module ports.

In this example, the **ikon_eth_util --all-pass-through** utility will validate the following connections between the F-ports, A-ports, B-ports, and C-ports. Figure 43 on page 1007 provides the ports that are validated in this example.

Table 101: Validating Ports

F-Ports	A-Ports	B-Ports	C-Ports
xe-0/0/10:2 This interface is one of the 10-Gigabit Ethernet ports on the QFX5100-24Q-AA switch. You can manage these ports through the Junos OS.	xe-0/0/32 This interface connects the PFE of the QFX5100-24Q-AA switch to the B-ports on the FPGA module on the QFX-PFA-4Q module.	JDFE_XE32_10G This interface is an Internal 10-Gigabit Ethernet port on the FPGA module on the QFX-PFA-4Q module and connects to the A-ports on the PFE of the QFX5100-24Q-AA switch.	JDFE_QSFP0_10G_PORT0 [External Port 0-0] This interface is one of the front-facing 40-Gigabit Ethernet ports on the QFX-PFA-4Q module and connects to the guest VM running on the QFX5100-24Q-AA switch and the F-ports on the QFX5100-24Q-AA switch.

To validate the connections between the QFX5100-24Q-AA switch network ports and the QFX-PFA-4Q module ports:

1. Configure a VLAN and VLAN ID:

```
[edit vlans]
user@switch # set VLAN_TEST vlan-id 100
```

2. Associate the F-port and A-port in this VLAN so that the FPGA and PFE can communicate:

```
[edit interfaces]
user@switch # set xe-0/0/10:2 unit 0 family ethernet-switching vlan members VLAN_TEST
user@switch # set xe-0/0/32 unit 0 family ethernet-switching vlan members VLAN_TEST
```

3. Commit the configuration:

```
[edit]
user@switch # commit synchronize
```

4. Verify that the VLAN has been created.

```
[edit]
user@switch # run show vlans
```

```
    Routing instance        VLAN name             Tag          Interfaces
    default-switch          VLAN_TEST              100
                                                               xe-0/0/10:2.0*
                                                               xe-0/0/32.0*
    default-switch          default               1
```

5. Issue the **ikon_eth_util --all-pass-through** command at the guest VM login prompt:

```
[root@ikondiag ~]# ikon_eth_util --all-pass-through
```

```
Ikon Ethernet Pass Through Utility
setting portConnect_JDFE_QSFP0_10G_PORT0_JDFE_XE32_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT1_JDFE_XE33_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT2_JDFE_XE34_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT3_JDFE_XE35_10G to 1
setting portConnect_JDFE_XE24_10G_JDFE_QSFP1_10G_PORT0 to 1
setting portConnect_JDFE_XE25_10G_JDFE_QSFP1_10G_PORT1 to 1
setting portConnect_JDFE_XE26_10G_JDFE_QSFP1_10G_PORT2 to 1
setting portConnect_JDFE_XE27_10G_JDFE_QSFP1_10G_PORT3 to 1
setting portConnect_JDFE_XE28_10G_JDFE_QSFP2_10G_PORT0 to 1
setting portConnect_JDFE_XE29_10G_JDFE_QSFP2_10G_PORT1 to 1
setting portConnect_JDFE_XE30_10G_JDFE_QSFP2_10G_PORT2 to 1
setting portConnect_JDFE_XE31_10G_JDFE_QSFP2_10G_PORT3 to 1
setting portConnect_JDFE_XE36_10G_JDFE_QSFP3_10G_PORT0 to 1
setting portConnect_JDFE_XE37_10G_JDFE_QSFP3_10G_PORT1 to 1
setting portConnect_JDFE_XE38_10G_JDFE_QSFP3_10G_PORT2 to 1
setting portConnect_JDFE_XE39_10G_JDFE_QSFP3_10G_PORT3 to 1
running press return key to exit
```

6. Send traffic to xe-0/0/10:2 on the QFX5100-24Q-AA switch and receive traffic on the front panel port 0-0 on the QFX-PFA-4Q module.

7. Send traffic to the front panel port 0-0 on the QFX-PFA-4Q module and receive traffic on xe-0/0/10:2 on the QFX5100-24Q-AA switch.

8. Verify the statistics for the xe-0/0/10:2 and xe-0/0/32 interfaces by issuing the **show interfaces xe-0/0/10:2 extensive** and **show interfaces xe-0/0/32 extensive** commands.

9. Verify the statistics for the JDFE_XE32_10G and JDFE_QSFP0_10G_PORT0 interfaces by issuing the **maxnet link** commands at the guest VM prompt for the Packet Flow Accelerator Diagnostics software.

[root@ikondiag ~]# **maxnet link show JDFE_XE32_10G**

```
JDFE_XE32_10G:
         Link Up: true
     MAC address: 00:11:22:33:44:55
      RX Enabled: true
       RX Frames: 1 ok
                  0 error
                  0 CRC error
                  0 invalid/errored
                  1 total
      TX Enabled: true
       TX Frames: 0 ok
                  0 error
                  0 CRC error
                  0 invalid/errored
                  0 total
```

[root@ikondiag ~]# **maxnet link show JDFE_QSFP0_10G_PORT0**

```
JDFE_QSFP0_10G_PORT0:
         Link Up: true
     MAC address: 00:11:22:33:44:55
      RX Enabled: true
       RX Frames: 0 ok
                  0 error
                  0 CRC error
                  0 invalid/errored
                  0 total
      TX Enabled: true
       TX Frames: 1 ok
                  0 error
                  0 CRC error
                  0 invalid/errored
                  1 total
```

Uninstalling the Guest VM

To remove the guest VM:

1. Delete the configuration statements and uninstall the Packet Flow Accelerator Diagnostics software package.

   For example, to remove the **app-engine** statement:

   ```
   root # delete services app-engine
   ```

2. Commit the configuration.

   ```
   root# commit
   ```

3. (Optional) Issue the **show version** command to learn the name of the Packet Flow Accelerator Diagnostics software package.

   ```
   {master:0}
   root> show version
   fpc0:

   --------------------------------------------------------------------------

   Hostname: switch

   Model: qfx5100-24q-aa

   Junos: 14.1X53-D27_vjunos.62

   JUNOS Base OS Software Suite [14.1X53-D27_vjunos.62]

   JUNOS Base OS boot [14.1X53-D27_vjunos.62]

   JUNOS Crypto Software Suite [14.1X53-D27_vjunos.62]

   JUNOS Online Documentation [14.1X53-D27_vjunos.62]
   ```

```
JUNOS Kernel Software Suite [14.1X53-D27_vjunos.62]

JUNOS Packet Forwarding Engine Support (qfx-ex-x86-32) [14.1X53-D26_vjunos.62]

JUNOS Routing Software Suite [14.1X53-D27_vjunos.62]

JUNOS Enterprise Software Suite [14.1X53-D27_vjunos.62]

JUNOS py-base-i386 [14.1X53-D27_vjunos.62]

JUNOS py-extensions-i386 [14.1X53-D27_vjunos.62]

JUNOS Host Software [14.1X53-D27_vjunos.62]

Junos for Automation Enhancement

JUNOS GUEST-VM Software [pfadiag_vm-rXXXXX-ve]



{master:0}
```

4. Issue the **request system software delete virtual-machine-package <*package-name*>** command to uninstall the Packet Flow Accelerator Diagnostics software.

   `root>` **request system software delete virtual-machine-package pfadiag_vm-rXXXXX-ve**

```
fpc0:
--------------------------------------------------------------------------
Deleted virtual-machine package dpfadiag_vm-rXXXXX-ve ...
```

RELATED DOCUMENTATION

- Understanding Packet Flow Accelerator Diagnostics Software and Other Utilities | **1006**
- *Installing an Expansion Module in a QFX5100 Device*
- Installing Ethernet and PTP Scripts | **1036**
- *Launching a Guest Virtual Machine (VM) to Run a Third Party Application on Junos OS Release 13.2X51-D20 and Later*
- *Installing Software Packages on QFX Series Devices*

8

PART

Monitoring Common Security Features

Displaying Real-Time Information from Device to Host | **1057**

Monitoring Security Policies | **1064**

Monitoring Interfaces and Switching Functions | **1096**

Monitoring Events, Services and System | **1103**

Monitoring Unified Threat Management Features | **1110**

CHAPTER 29

Displaying Real-Time Information from Device to Host

IN THIS CHAPTER

- Displaying Real-Time Monitoring Information | 1057
- Displaying Multicast Path Information | 1060

Displaying Real-Time Monitoring Information

To display real-time monitoring information about each device between the device and a specified destination host, enter the **traceroute monitor** command with the following syntax:

```
user@host> traceroute monitor host <count number> <inet | inet6> <interval seconds> <no-resolve> <size
  bytes><source source-address> <summary>
```

Table 102 on page 1057 describes the **traceroute monitor** command options.

Table 102: CLI traceroute monitor Command Options

Option	Description
host	Sends traceroute packets to the hostname or IP address you specify.
count *number*	(Optional) Limits the number of ping requests, in packets, to send in summary mode. If you do not specify a count, ping requests are continuously sent until you press Q.
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.
interval *seconds*	(Optional) Sets the interval between ping requests, in seconds. The default value is **1** second.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.

Table 102: CLI traceroute monitor Command Options *(continued)*

Option	Description
size *bytes*	(Optional) Sets the size of the ping request packet. The size can be from **0** through **65,468** bytes. The default packet size is **64** bytes.
source ***address***	(Optional) Uses the source address that you specify, in the traceroute packet.
summary	(Optional) Displays the summary traceroute information.

To quit the **traceroute monitor** command, press Q.

The following is sample output from a **traceroute monitor** command:

```
user@host> traceroute monitor host2
```

```
                                                  My traceroute  [v0.69]
host (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)
                        Wed Mar 14 23:14:11 2007
Keys:  Help   Display mode   Restart statistics   Order of fields   quit

          Packets               Pings
 Host
       Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 173.24.232.66
        0.0%     5    9.4   8.6   4.8   9.9   2.1
 2. 173.24.232.66
        0.0%     5    7.9  17.2   7.9  29.4  11.0
 3. 173.24.232.66
        0.0%     5    9.9   9.3   8.7   9.9   0.5
 4. 173.24.232.66
        0.0%     5    9.9   9.8   9.5  10.0   0.2
```

Table 103 on page 1058 summarizes the output fields of the display.

Table 103: CLI traceroute monitor Command Output Summary

Field	Description
host	Hostname or IP address of the device issuing the **traceroute monitor** command.
psize*size*	Size of ping request packet, in bytes.

Table 103: CLI traceroute monitor Command Output Summary *(continued)*

Field	Description
Keys	
Help	Displays the Help for the CLI commands. Press H to display the Help.
Display mode	Toggles the display mode. Press D to toggle the display mode
Restart statistics	Restarts the **traceroute monitor** command. Press R to restart the **traceroute monitor** command.
Order of fields	Sets the order of the displayed fields. Press O to set the order of the displayed fields.
quit	Quits the **traceroute monitor** command. Press Q to quit the **traceroute monitor** command.
Packets	
number	Number of the hop (device) along the route to the final destination host.
Host	Hostname or IP address of the device at each hop.
Loss%	Percent of packet loss. The number of ping responses divided by the number of ping requests, specified as a percentage.
Pings	
Snt	Number of ping requests sent to the device at this hop.
Last	Most recent round-trip time, in milliseconds, to the device at this hop.
Avg	Average round-trip time, in milliseconds, to the device at this hop.
Best	Shortest round-trip time, in milliseconds, to the device at this hop.
Wrst	Longest round-trip time, in milliseconds, to the device at this hop.
StDev	Standard deviation of round-trip times, in milliseconds, to the device at this hop.

RELATED DOCUMENTATION

Displaying Log and Trace Files | 1634

Displaying Multicast Path Information

To display information about a multicast path from a source to the device, enter the **mtrace from-source** command with the following syntax:

```
user@host> mtrace from-source source host <extra-hops number> <group address> <interval seconds>
   <max-hops number> <max-queries number> <response host> <routing-instance routing-instance-name>
   <ttl number> <wait-time seconds> <loop> <multicast-response | unicast-response> <no-resolve>
   <no-router-alert> <brief | detail>
```

Table 104 on page 1060 describes the **mtrace from-source** command options.

Table 104: CLI mtrace from-source Command Options

Option	Description
source *host*	Traces the path to the specified hostname or IP address.
extra-hops *number*	(Optional) Sets the number of extra hops to trace past nonresponsive devices. Specify a value from **0** through **255**.
group *address*	(Optional) Traces the path for the specified group address. The default value is **192.0.2.0**.
interval *seconds*	(Optional) Sets the interval between statistics gathering. The default value is **10**.
max-hops *number*	(Optional) Sets the maximum number of hops to trace toward the source. Specify a value from **0** through **255**. The default value is **32**.
max-queries *number*	(Optional) Sets the maximum number of query attempts for any hop. Specify a value from **1** through **32**. The default value is **3**.
response *host*	(Optional) Sends the response packets to the specified hostname or IP address. By default, the response packets are sent to the device.
routing-instance *routing-instance-name*	(Optional) Traces the routing instance you specify.

Table 104: CLI mtrace from-source Command Options *(continued)*

Option	Description
ttl *number*	(Optional) Sets the time-to-live (TTL) value in the IP header of the query packets. Specify a hop count from **0** through **255**. The default value for local queries to the ***all routers*** multicast group is **1**. Otherwise, the default value is **127**.
wait-time *seconds*	(Optional) Sets the time to wait for a response packet. The default value is **3** seconds.
loop	(Optional) Loops indefinitely, displaying rate and loss statistics. To quit the **mtrace** command, press Ctrl-C.
multicast-response	(Optional) Forces the responses to use multicast.
unicast-response	(Optional) Forces the response packets to use unicast.
no-resolve	(Optional) Does not display hostnames.
no-router-alert	(Optional) Does not use the device alert IP option in the IP header.
brief	(Optional) Does not display packet rates and losses.
detail	(Optional) Displays packet rates and losses if a group address is specified.

The following is sample output from the **mtrace from-source** command:

```
user@host> mtrace from-source source 192.1.4.1 group 224.1.1.1
```

```
Mtrace from 192.1.4.1 to 192.1.30.2 via group 224.1.1.1 Querying full reverse
path... * *    0  ? (192.1.30.2)  -1  ? (192.1.30.1)  PIM  thresh^ 1    -2
routerC.mycompany.net (192.1.40.2)  PIM  thresh^ 1    -3  hostA.mycompany.net
(192.1.4.1) Round trip time 22 ms; total ttl of 2 required.  Waiting to accumulate
 statistics...Results after 10 seconds:    Source        Response Dest    Overall
     Packet Statistics For Traffic From 192.1.4.1  192.1.30.2       Packet
192.1.4.1 To 224.1.1.1      v       __/  rtt   16 ms     Rate       Lost/Sent =
Pct  Rate 192.168.195.37  192.1.40.2      routerC.mycompany.net       v     ^
  ttl    2                    0/0    = --    0 pps 192.1.40.1      192.1.30.1
    ?                  v      \__   ttl    3                     ?/0
  0 pps 192.1.30.2      192.1.30.2   Receiver      Query Source
```

Each line of the trace display is usually in the following format (depending on the options selected and the responses from the devices along the path):

```
hop-number host (ip-address) protocolttl
```

Table 105 on page 1062 summarizes the output fields of the display.

> **NOTE:** The packet statistics gathered from Juniper Networks devices and routing nodes always display as **0**.

Table 105: CLI mtrace from-source Command Output Summary

Field	Description
hop-number	Number of the hop (device) along the path.
host	Hostname, if available, or IP address of the device. If the **no-resolve** option was entered in the command, the hostname is not displayed.
ip-address	IP address of the device.
protocol	Protocol used.
ttl	TTL threshold.
Round trip time *milliseconds* ms	Total time between the sending of the query packet and the receiving of the response packet.
total ttl of *number* required	Total number of hops required to reach the source.
Source	Source IP address of the response packet.
Response Dest	Response destination IP address.
Overall	Average packet rate for all traffic at each hop.
Packet Statistics For Traffic From	Number of packets lost, number of packets sent, percentage of packets lost, and average packet rate at each hop.
Receiver	IP address receiving the multicast packets.
Query Source	IP address of the host sending the query packets.

RELATED DOCUMENTATION

Monitoring Overview | 15

CHAPTER 30

Monitoring Security Policies

IN THIS CHAPTER

- Monitoring Security Policy Statistics | 1064
- Monitoring Routing Information | 1065
- Monitoring Security Events by Policy | 1074
- Monitoring Security Features | 1077

Monitoring Security Policy Statistics

Purpose

Monitor and record traffic that Junos OS permits or denies based on previously configured policies.

Action

To monitor traffic, enable the count and log options.

Count—Configurable in an individual policy. If count is enabled, statistics are collected for sessions that enter the device for a given policy, and for the number of packets and bytes that pass through the device in both directions for a given policy. For counts (only for packets and bytes), you can specify that alarms be generated whenever the traffic exceeds specified thresholds. See count (Security Policies).

Log—Logging capability can be enabled with security policies during session initialization (**session-init**) or session close (**session-close**) stage. See log (Security Policies).

- To view logs from denied connections, enable log on **session-init**.
- To log sessions after their conclusion/tear-down, enable log on **session-close**.

> **NOTE:** Session log is enabled at real time in the flow code which impacts the user performance. If both **session-close** and **session-init** are enabled, performance is further degraded as compared to enabling **session-init** only.

For details about information collected for session logs, see *Information Provided in Session Log Entries for SRX Series Services Gateways*.

Monitoring Routing Information

IN THIS SECTION

- Monitoring Route Information | 1065
- Monitoring RIP Routing Information | 1068
- Monitoring OSPF Routing Information | 1069
- Monitoring BGP Routing Information | 1072

This section contains the following topics:

Monitoring Route Information

Purpose

View information about the routes in a routing table, including destination, protocol, state, and parameter information.

Action

Select **Monitor>Routing>Route Information** in the J-Web user interface, or enter the following CLI commands:

- **show route terse**
- **show route detail**

> **NOTE:** When you use an HTTPS connection in the Microsoft Internet Explorer browser to save a report from this page in the J-Web interface, the error message "Internet Explorer was not able to open the Internet site" is displayed. This problem occurs because the Cache-Control: no cache HTTP header is added on the server side and Internet Explorer does not allow you to download the encrypted file with the Cache-Control: no cache HTTP header set in the response from the server.
>
> As a workaround, refer to Microsoft Knowledge Base article 323308, which is available at this URL: http://support.microsoft.com/kb/323308. Also, you can alternatively use HTTP in the Internet Explorer browser or use HTTPS in the Mozilla Firefox browser to save a file from this page.

Table 106 on page 1066 describes the different filters, their functions, and the associated actions.

Table 107 on page 1066 summarizes key output fields in the routing information display.

Table 106: Filtering Route Messages

Field	Function	Your Action
Destination Address	Specifies the destination address of the route.	Enter the destination address.
Protocol	Specifies the protocol from which the route was learned.	Enter the protocol name.
Next hop address	Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	Enter the next hop address.
Receive protocol	Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.	Enter the routing protocol.
Best route	Specifies only the best route available.	Select the view details of the best route.
Inactive routes	Specifies the inactive routes.	Select the view details of inactive routes.
Exact route	Specifies the exact route.	Select the view details of the exact route.
Hidden routes	Specifies the hidden routes.	Select the view details of hidden routes.
Search	Applies the specified filter and displays the matching messages.	To apply the filter and display messages, click **Search**.
Reset	Resets selected options to default	To reset the filter, click **Reset**.

Table 107: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
Static Route Addresses	The list of static route addresses.	–
Protocol	Protocol from which the route was learned: **Static**, **Direct**, **Local**, or the name of a particular protocol.	–

Table 107: Summary of Key Routing Information Output Fields *(continued)*

Field	Values	Additional Information
Preference	The preference is the individual preference value for the route.	The route preference is used as one of the route selection criteria.
Next-Hop	Network Layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	If a next hop is listed as **Discard**, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the **discard** attribute has been set. If a next hop is listed as **Reject**, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected. If a next hop is listed as **Local**, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).
Age	How long the route has been active.	–
State	Flags for this route.	There are many possible flags.
AS Path	AS path through which the route was learned. The letters of the AS path indicate the path origin: • **I**—IGP. • **E**—EGP. • **?**—Incomplete. Typically, the AS path was aggregated.	–

SEE ALSO

Monitoring RIP Routing Information | 1068

Monitoring OSPF Routing Information | 1069

Monitoring BGP Routing Information | 1072

Monitoring RIP Routing Information

Purpose

View RIP routing information, including a summary of RIP neighbors and statistics.

Action

Select **Monitor>Routing>RIP Information** in the J-Web user interface, or enter the following CLI commands:

- **show rip statistics**
- **show rip neighbors**

Table 108 on page 1068 summarizes key output fields in the RIP routing display in the J-Web user interface.

Table 108: Summary of Key RIP Routing Output Fields

Field	Values	Additional Information
RIP Statistics		
Protocol Name	The RIP protocol name.	–
Port number	The port on which RIP is enabled.	–
Hold down time	The interval during which routes are neither advertised nor updated.	–
Global routes learned	Number of RIP routes learned on the logical interface.	–
Global routes held down	Number of RIP routes that are not advertised or updated during the hold-down interval.	–
Global request dropped	Number of requests dropped.	–
Global responses dropped	Number of responses dropped.	–
RIP Neighbors		
Details	Tab used to view the details of the interface on which RIP is enabled.	–
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor.

Table 108: Summary of Key RIP Routing Output Fields *(continued)*

Field	Values	Additional Information
State	State of the RIP connection: **Up** or **Dn** (Down).	–
Source Address	Local source address.	This value is the configured address of the interface on which RIP is enabled.
Destination Address	Destination address.	This value is the configured address of the immediate RIP adjacency.
Send Mode	The mode of sending RIP messages.	–
Receive Mode	The mode in which messages are received.	–
In Metric	Value of the incoming metric configured for the RIP neighbor.	–

SEE ALSO

Monitoring Route Information | 1065

Monitoring OSPF Routing Information | 1069

Monitoring BGP Routing Information | 1072

Monitoring OSPF Routing Information

Purpose

View OSPF routing information, including a summary of OSPF neighbors, interfaces, and statistics.

Action

Select **Monitor>Routing>OSPF Information** in the J-Web user interface, or enter the following CLI commands:

- **show ospf neighbors**
- **show ospf interfaces**
- **show ospf statistics**

Table 109 on page 1070 summarizes key output fields in the OSPF routing display in the J-Web user interface.

Table 109: Summary of Key OSPF Routing Output Fields

Field	Values	Additional Information
OSPF Interfaces		
Details	Tab used to view the details of the selected OSPF.	–
Interface	Name of the interface running OSPF.	–
State	State of the interface: **BDR**, **Down**, **DR**, **DRother**, **Loop**, **PtToPt**, or **Waiting**.	The **Down** state, indicating that the interface is not functioning, and **PtToPt** state, indicating that a point-to-point connection has been established, are the most common states.
Area	Number of the area that the interface is in.	–
DR ID	ID of the area's designated device.	–
BDR ID	ID of the area's backup designated device.	–
Neighbors	Number of neighbors on this interface.	–
OSPF Statistics		
Packets tab		
Sent	Displays the total number of packets sent.	–
Received	Displays the total number of packets received.	–
Details tab		
Flood Queue Depth	Number of entries in the extended queue.	–
Total Retransmits	Number of retransmission entries enqueued.	–
Total Database Summaries	Total number of database description packets.	–
OSPF Neighbors		
Address	Address of the neighbor.	–

Table 109: Summary of Key OSPF Routing Output Fields *(continued)*

Field	Values	Additional Information
Interface	Interface through which the neighbor is reachable.	–
State	State of the neighbor: **Attempt**, **Down**, **Exchange**, **ExStart**, **Full**, **Init**, **Loading**, or **2way**.	Generally, only the **Down** state, indicating a failed OSPF adjacency, and the **Full** state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.
ID	ID of the neighbor.	–
Priority	Priority of the neighbor to become the designated router.	–
Activity Time	The activity time.	–
Area	Area that the neighbor is in.	–
Options	Option bits received in the hello packets from the neighbor.	–
DR Address	Address of the designated router.	–
BDR Address	Address of the backup designated router.	–
Uptime	Length of time since the neighbor came up.	–
Adjacency	Length of time since the adjacency with the neighbor was established.	–

SEE ALSO

Monitoring Route Information | 1065

Monitoring RIP Routing Information | 1068

Monitoring BGP Routing Information | 1072

Monitoring BGP Routing Information

Purpose

Monitor BGP routing information on the routing device, including a summary of BGP routing and neighbor information.

Action

Select **Monitor>Routing>BGP Information** in the J-Web user interface, or enter the following CLI commands:

- **show bgp summary**
- **show bgp neighbor**

Table 110 on page 1072 summarizes key output fields in the BGP routing display in the J-Web user interface.

Table 110: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Peer Summary		
Total Groups	Number of BGP groups.	–
Total Peers	Number of BGP peers.	–
Down Peers	Number of unavailable BGP peers.	–
Unconfigured Peers	Address of each BGP peer.	–
RIB Summary tab		
RIB Name	Name of the RIB group.	–
Total Prefixes	Total number of prefixes from the peer, both active and inactive, that are in the routing table.	–
Active Prefixes	Number of prefixes received from the EBGP peers that are active in the routing table.	–
Suppressed Prefixes	Number of routes received from EBGP peers currently inactive because of damping or other reasons.	–
History Prefixes	History of the routes received or suppressed.	–

Table 110: Summary of Key BGP Routing Output Fields *(continued)*

Field	Values	Additional Information
Dumped Prefixes	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.	–
Pending Prefixes	Number of pending routes.	–
State	Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.	–
BGP Neighbors		
Details	Click this button to view the selected BGP neighbor details.	–
Peer Address	Address of the BGP neighbor.	–
Autonomous System	AS number of the peer.	–
Peer State	Current state of the BGP session: • **Active**—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. • **Connect**—BGP is waiting for the TCP connection to become complete. • **Established**—The BGP session has been established, and the peers are exchanging BGP update messages. • **Idle**—This is the first stage of a connection. BGP is waiting for a Start event. • **OpenConfirm**—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. • **OpenSent**—BGP has sent an open message and is waiting to receive an open message from the peer.	Generally, the most common states are **Active**, which indicates a problem establishing the BGP connection, and **Established**, which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time.

Table 110: Summary of Key BGP Routing Output Fields *(continued)*

Field	Values	Additional Information
Elapsed Time	Elapsed time since the peering session was last reset.	–
Description	Description of the BGP session.	–

SEE ALSO

- Monitoring Route Information | **1065**
- Monitoring RIP Routing Information | **1068**
- Monitoring OSPF Routing Information | **1069**

RELATED DOCUMENTATION

- Monitoring Overview | **15**
- Monitoring Interfaces | **1100**

Monitoring Security Events by Policy

Purpose

Monitor security events by policy and display logged event details with the J-Web user interface.

Action

To monitor security events by policy:

1. Select one of the following in the J-Web user interface:
   - If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Events and Alarms>Security Events**.
   - Select **Monitor>Alarms>Policy Log**.

   The View Policy Log pane appears. Table 111 on page 1075 describes the content of this pane.

Table 111: View Policy Log Fields

Field	Value
Log file name	Name of the event log files to search.
Policy name	Name of the policy of the events to be retrieved.
Source address	Source address of the traffic that triggered the event.
Destination address	Destination address of the traffic that triggered the event.
Event type	Type of event that was triggered by the traffic.
Application	Application of the traffic that triggered the event.
Source port	Source port of the traffic that triggered the event.
Destination port	Destination port of the traffic that triggered the event.
Source zone	Source zone of the traffic that triggered the event.
Destination zone	Destination zone of the traffic that triggered the event.
Source NAT rule	Source NAT rule of the traffic that triggered the event.
Destination NAT rule	Destination NAT rule of the traffic that triggered the event.
Is global policy	Specifies that the policy is a global policy.

If your device is not configured to store session log files locally, the Create log configuration button is displayed in the lower-right portion of the View Policy Log pane.

- To store session log files locally, click **Create log configuration**.

If session logs are being sent to an external log collector (stream mode has been configured for log files), a message appears indicating that event mode must be configured to view policy logs.

> **NOTE:** Reverting to event mode will discontinue event logging to the external log collector.

- To reset the **mode** option to **event**, enter the **set security log** command.

2. Enter one or more search fields in the View Policy Log pane and click **Search** to display events matching your criteria.

For example, enter the event type **Session Close** and the policy **pol1** to display event details from all Session Close logs that contain the specified policy. To reduce search results further, add more criteria about the particular event or group of events that you want displayed.

The Policy Events Detail pane displays information from each matching session log. Table 112 on page 1076 describes the contents of this pane.

Table 112: Policy Events Detail Fields

Field	Value
Timestamp	Time when the event occurred.
Policy name	Policy that triggered the event.
Record type	Type of event log providing the data.
Source IP/Port	Source address (and port, if applicable) of the event traffic.
Destination IP/Port	Destination address (and port, if applicable) of the event traffic.
Service name	Service name of the event traffic.
NAT source IP/Port	NAT source address (and port, if applicable) of the event traffic.
NAT destination IP/Port	NAT destination address (and port, if applicable) of the event traffic.

RELATED DOCUMENTATION

Monitoring Overview | **15**

Monitoring Interfaces | **1100**

Monitoring Alarms

Monitoring Events

Monitoring Security Features

IN THIS SECTION

- Monitoring Policies | 1077
- Checking Policies | 1080
- Monitoring Screen Counters | 1083
- Monitoring IDP Status | 1086
- Monitoring Flow Gate Information | 1088
- Monitoring Firewall Authentication Table | 1089
- Monitoring Firewall Authentication History | 1091
- Monitoring 802.1x | 1093

This section contains the following topics:

Monitoring Policies

Purpose

Display, sort, and review policy activity for every activated policy configured on the device. Policies are grouped by Zone Context (the from and to zones of the traffic) to control the volume of data displayed at one time. From the policy list, select a policy to display statistics and current network activity.

Action

To review policy activity:

1. Select **Monitor>Security>Policy>Activities** in the J-Web user interface. The Security Policies Monitoring page appears and lists the policies from the first Zone Context. See Table 113 on page 1078 for field descriptions.
2. Select the **Zone Context** of the policy you want to monitor, and click **Filter**. All policies within the zone context appear in match sequence.
3. Select a policy, and click **Clear Statistics** to set all counters to zero for the selected policy.

Table 113: Security Policies Monitoring Output Fields

Field	Value	Additional Information
Zone Context (Total #)	Displays a list of all from and to zone combinations for the configured policies. The total number of active policies for each context is specified in the Total # field. By default, the policies from the first Zone Context are displayed.	To display policies for a different context, select a zone context and click **Filter**. Both inactive and active policies appear for each context. However, the Total # field for a context specifies the number of active policies only.
Default Policy action	Specifies the action to take for traffic that does not match any of the policies in the context: • permit-all—Permit all traffic that does not match a policy. • deny-all—Deny all traffic that does not match a policy.	–
From Zone	Displays the source zone to be used as match criteria for the policy.	–
To Zone	Displays the destination zone to be used as match criteria for the policy.	–
Name	Displays the name of the policy.	–
Source Address	Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. (In this case, only the names are given, not the IP addresses).	–
Destination Address	Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book.	–
Source Identity	Displays the name of the source identities set for the policy.	To display the value of the source identities, hover the mouse on this field. Unknown source identities are also displayed.
Application	Displays the name of a predefined or custom application signature to be used as match criteria for the policy.	–

Table 113: Security Policies Monitoring Output Fields *(continued)*

Field	Value	Additional Information
Dynamic App	Displays the dynamic application signatures to be used as match criteria if an application firewall rule set is configured for the policy. For a network firewall, a dynamic application is not defined.	The rule set appears in two lines. The first line displays the configured dynamic application signatures in the rule set. The second line displays the default dynamic application signature. If more than two dynamic application signatures are specified for the rule set, hover over the output field to display the full list in a tooltip.
Action	Displays the action portion of the rule set if an application firewall rule set is configured for the policy. • permit—Permits access to the network services controlled by the policy. A green background signifies permission. • deny—Denies access to the network services controlled by the policy. A red background signifies denial.	The action portion of the rule set appears in two lines. The first line identifies the action to be taken when the traffic matches a dynamic application signature. The second line displays the default action when traffic does not match a dynamic application signature.
NW Services	Displays the network services permitted or denied by the policy if an application firewall rule set is configured. Network services include: • gprs-gtp-profile—Specify a GPRS Tunneling Protocol profile name. • idp—Perform intrusion detection and prevention. • redirect-wx—Set WX redirection. • reverse-redirect-wx—Set WX reverse redirection. • uac-policy—Enable unified access control enforcement of the policy.	–
Policy Hit Counters Graph	Provides a representation of the value over time for a specified counter. The graph is blank if Policy Counters indicates no data. As a selected counter accumulates data, the graph is updated at each refresh interval.	To toggle a graph on and off, click the counter name below the graph.

Table 113: Security Policies Monitoring Output Fields *(continued)*

Field	Value	Additional Information
Policy Counters	Lists statistical counters for the selected policy if Count is enabled. The following counters are available for each policy: • input-bytes • input-byte-rate • output-bytes • output-byte-rate • input-packets • input-packet-rate • output-packets • output-packet-rate • session-creations • session-creation-rate • active-sessions	To graph or to remove a counter from the Policy Hit Counters Graph, toggle the counter name. The names of enabled counters appear below the graph.

SEE ALSO

Checking Policies | 1080

Monitoring Screen Counters | 1083

Checking Policies

Purpose

Enter match criteria and conduct a policy search. The search results include all policies that match the traffic criteria in the sequence in which they will be encountered.

Because policy matches are listed in the sequence in which they would be encountered, you can determine whether a specific policy is being applied correctly or not. The first policy in the list is applied to all matching traffic. Policies listed after this one remain in the “shadow” of the first policy and are never encountered by this traffic.

By manipulating the traffic criteria and policy sequence, you can tune policy application to suit your needs. During policy development, you can use this feature to establish the appropriate sequence of policies for optimum traffic matches. When troubleshooting, use this feature to determine if specific traffic is encountering the appropriate policy.

Action

1. Select **Monitor>Security>Policy>Shadow Policies** in the J-Web user interface. The Check Policies page appears. Table 114 on page 1081 explains the content of this page.

2. In the top pane, enter the From Zone and To Zone to supply the context for the search.

3. Enter match criteria for the traffic, including the source address and port, the destination address and port, and the protocol of the traffic.

4. Enter the number of matching policies to display.

5. Click **Search** to find policies matching your criteria. The lower pane displays all policies matching the criteria up to the number of policies you specified.
   - The first policy will be applied to all traffic with this match criteria.
   - Remaining policies will not be encountered by any traffic with this match criteria.
6. To manipulate the position and activation of a policy, select the policy and click the appropriate button:
   - **Move**—Moves the selected policy up or down to position it at a more appropriate point in the search sequence.
   - **Move to**—Moves the selected policy by allowing you to drag and drop it to a different location on the same page.

Table 114: Check Policies Output

Field	Function
Check Policies Search Input Pane	
From Zone	Name or ID of the source zone. If a From Zone is specified by name, the name is translated to its ID internally.
To Zone	Name or ID of the destination zone. If a To Zone is specified by name, the name is translated to its ID internally.
Source Address	Address of the source in IP notation.
Source Port	Port number of the source.
Destination Address	Address of the destination in IP notation.
Destination Port	Port number of the destination.
Source Identity	Name of the source identity.

Table 114: Check Policies Output *(continued)*

Field	Function
Protocol	Name or equivalent value of the protocol to be matched. **ah**—51 **egp**—8 **esp**—50 **gre**—47 **icmp**—1 **igmp**—2 **igp**—9 **ipip**—94 **ipv6**—41 **ospf**—89 **pgm**—113 **pim**—103 **rdp**—27 **rsvp**—46 **sctp**—132 **tcp**—6 **udp**—17 **vrrp**—112
Result Count	(Optional) Number of policies to display. Default value is 1. Maximum value is 16.
Check Policies List	
From Zone	Name of the source zone.
To Zone	Name of the destination zone.
Total Policies	Number of policies retrieved.

Table 114: Check Policies Output *(continued)*

Field	Function
Default Policy action	The action to be taken if no match occurs.
Name	Policy name
Source Address	Name of the source address (not the IP address) of a policy. Address sets are resolved to their individual names.
Destination Address	Name of the destination address or address set. A packet's destination address must match this value for the policy to apply to it.
Source Identity	Name of the source identity for the policy.
Application	Name of a preconfigured or custom application of the policy match.
Action	Action taken when a match occurs as specified in the policy.
Hit Counts	Number of matches for this policy. This value is the same as the Policy Lookups in a policy statistics report.
Active Sessions	Number of active sessions matching this policy.

Alternatively, to list matching policies using the CLI, enter the **show security match-policies** command and include your match criteria and the number of matching policies to display.

SEE ALSO

Monitoring Policies | **1077**
Monitoring Screen Counters | **1083**

Monitoring Screen Counters

Purpose

View screen statistics for a specified security zone.

Action

Select **Monitor>Security>Screen Counters** in the J-Web user interface, or enter the following CLI command:

show security screen statistics zone *zone-name*

Table 115 on page 1084 summarizes key output fields in the screen counters display.

Table 115: Summary of Key Screen Counters Output Fields

Field	Values	Additional Information
Zones		
ICMP Flood	Internet Control Message Protocol (ICMP) flood counter.	An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP Flood	User Datagram Protocol (UDP) flood counter.	UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP Winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks.	WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP Port Scan	Number of TCP port scans.	The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP Address Sweep	Number of ICMP address sweeps.	An IP address sweep can occur with the intent of triggering responses from active hosts.
IP Tear Drop	Number of teardrop attacks.	Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN Attack	Number of TCP SYN attacks.	–
IP Spoofing	Number of IP spoofs.	IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP Ping of Death	ICMP ping of death counter.	Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP Source Route	Number of IP source route attacks.	–

Table 115: Summary of Key Screen Counters Output Fields *(continued)*

Field	Values	Additional Information
TCP Land Attack	Number of land attacks.	Land attacks occur when attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN Fragment	Number of TCP SYN fragments.	–
TCP No Flag	Number of TCP headers without flags set.	A normal TCP segment header has at least one control flag set.
IP Unknown Protocol	Number of unknown Internet protocols.	–
IP Bad Options	Number of invalid options.	–
IP Record Route Option	Number of packets with the IP record route option enabled.	This option records the IP addresses of the network devices along the path that the IP packet travels.
IP Timestamp Option	Number of IP timestamp option attacks.	This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP Security Option	Number of IP security option attacks.	–
IP Loose route Option	Number of IP loose route option attacks.	This option specifies a partial route list for a packet to take on its journey from source to destination.
IP Strict Source Route Option	Number of IP strict source route option attacks.	This option specifies the complete route list for a packet to take on its journey from source to destination.
IP Stream Option	Number of stream option attacks.	This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.

Table 115: Summary of Key Screen Counters Output Fields *(continued)*

Field	Values	Additional Information
ICMP Fragment	Number of ICMP fragments.	Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP Large Packet	Number of large ICMP packets.	–
TCP SYN FIN Packet	Number of TCP SYN FIN packets.	–
TCP FIN without ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.	–
TCP SYN-ACK-ACK Proxy	Number of TCP flags enabled with SYN-ACK-ACK.	To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, Junos OS rejects further connection requests from that IP address.
IP Block Fragment	Number of IP block fragments.	–

SEE ALSO

Monitoring Policies | **1077**

Checking Policies | **1080**

Monitoring IDP Status

Purpose

View detailed information about the IDP Status, Memory, Counters, Policy Rulebase Statistics, and Attack table statistics.

Action

To view Intrusion Detection and Prevention (IDP) table information, do one of the following:

- If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Security>IDP>Status** in the J-Web user interface, or enter the following CLI commands:

show security idp status

show security idp memory

- Select **Monitor>Security>IPS>Status** in the J-Web user interface.

Table 116 on page 1087 summarizes key output fields in the IDP display.

Table 116: Summary of IDP Status Output Fields

Field	Values	Additional Information
IDP Status		
Status of IDP	Displays the status of the current IDP policy.	–
Up Since	Displays the time from when the IDP policy first began running on the system.	–
Packets/Second	Displays the number of packets received and returned per second.	–
Peak	Displays the maximum number of packets received per second and the time when the maximum was reached.	–
Kbits/Second	Displays the aggregated throughput (kilobits per second) for the system.	–
Peak Kbits	Displays the maximum kilobits per second and the time when the maximum was reached.	–
Latency (Microseconds)	Displays the delay, in microseconds, for a packet to receive and return by a node .	–
Current Policy	Displays the name of the current installed IDP policy.	–
IDP Memory Status		
IDP Memory Statistics	Displays the status of all IDP data plane memory.	–
PIC Name	Displays the name of the PIC.	–

Table 116: Summary of IDP Status Output Fields *(continued)*

Field	Values	Additional Information
Total IDP Data Plane Memory (MB)	Displays the total memory space, in megabytes, allocated for the IDP data plane.	–
Used (MB)	Displays the used memory space, in megabytes, for the data plane.	–
Available (MB)	Displays the available memory space, in megabytes, for the data plane.	–

SEE ALSO

Monitoring Flow Session Statistics

Monitoring Flow Gate Information

Purpose

View information about temporary openings known as pinholes or gates in the security firewall.

Action

Select **Monitor>Security>Flow Gate** in the J-Web user interface, or enter the **show security flow gate** command.

Table 117 on page 1088 summarizes key output fields in the flow gate display.

Table 117: Summary of Key Flow Gate Output Fields

Field	Values	Additional Information
Flow Gate Information		
Hole	Range of flows permitted by the pinhole.	–
Translated	Tuples used to create the session if it matches the pinhole: • Source address and port • Destination address and port	–
Protocol	Application protocol, such as UDP or TCP.	–
Application	Name of the application.	–

Table 117: Summary of Key Flow Gate Output Fields *(continued)*

Field	Values	Additional Information
Age	Idle timeout for the pinhole.	–
Flags	Internal debug flags for pinhole.	–
Zone	Incoming zone.	–
Reference count	Number of resource manager references to the pinhole.	–
Resource	Resource manager information about the pinhole.	–

SEE ALSO

Monitoring Flow Session Statistics

Monitoring Firewall Authentication

Monitoring Firewall Authentication Table

Purpose

View information about the authentication table, which divides firewall authentication user information into multiple parts.

Action

Select **Monitor>Security>Firewall Authentication>Authentication Table** in the J-Web user interface. To view detailed information about the user with a particular identifier, select the ID on the Authentication Table page. To view detailed information about the user at a particular source IP address, select the Source IP on the Authentication Table page.

Alternatively, enter the following CLI **show** commands:

- **show security firewall-authentication users**
- **show security firewall-authentication users address *ip-address***
- **show security firewall-authentication users identifier *identifier***

Table 118 on page 1090 summarizes key output fields in firewall authentication table display.

Table 118: Summary of Key Firewall Authentication Table Output Fields

Field	Values	Additional Information
Firewall authentication users		
Total users in table	Number of users in the authentication table.	–
Authentication table		
ID	Authentication identification number.	–
Source Ip	IP address of the authentication source.	–
Age	Idle timeout for the user.	–
Status	Status of authentication (**success** or **failure**).	–
user	Name of the user.	–
Detailed report per ID selected: *ID*		
Source Zone	Name of the source zone.	–
Destination Zone	Name of the destination zone.	–
profile	Name of the profile.	Users information.
Authentication method	Path chosen for authentication.	–
Policy Id	Policy Identifier.	–
Interface name	Name of the interface.	–
Bytes sent by this user	Number of packets in bytes sent by this user.	–
Bytes received by this user	Number of packets in bytes received by this user.	–
Client-groups	Name of the client group.	–
Detailed report per Source Ip selected		
Entries from Source IP	IP address of the authentication source.	–
Source Zone	Name of the source zone.	–

Table 118: Summary of Key Firewall Authentication Table Output Fields *(continued)*

Field	Values	Additional Information
Destination Zone	Name of the destination zone.	–
profile	Name of the profile.	–
Age	Idle timeout for the user.	–
Status	Status of authentication (**success** or **failure**).	–
user	Name of the user.	–
Authentication method	Path chosen for authentication.	–
Policy Id	Policy Identifier.	–
Interface name	Name of the interface.	–
Bytes sent by this user	Number of packets in bytes sent by this user.	–
Bytes received by this user	Number of packets in bytes received by this user.	–
Client-groups	Name of the client group.	–

Monitoring Firewall Authentication History

Purpose

View information about the authentication history, which is divided into multiple parts.

Action

Select **Monitor>Security>Firewall Authentication>Authentication History** in the J-Web user interface. To view the detailed history of the authentication with this identifier, select the ID on the Firewall Authentication History page. To view a detailed authentication history of this source IP address, select the Source IP on the Firewall Authentication History page.

Alternatively, enter the following CLI **show** commands:

- **show security firewall-authentication history**
- **show security firewall-authentication history address *ip-address***
- **show security firewall-authentication history identifier *identifier***

Table 119 on page 1092 summarizes key output fields in firewall authentication history display.

Table 119: Summary of Key Firewall Authentication History Output Fields

Field	Values	Additional Information
History of Firewall Authentication Data		
Total authentications	Number of authentication.	–
History Table		
ID	Identification number.	–
Source Ip	IP address of the authentication source.	–
Start Date	Authentication date.	–
Start Time	Authentication time.	–
Duration	Authentication duration.	–
Status	Status of authentication (**success** or **failure**).	–
User	Name of the user.	–
Detail history of selected Id: *ID*		
Authentication method	Path chosen for authentication.	–
Policy Id	Security policy identifier.	–
Source zone	Name of the source zone.	–
Destination Zone	Name of the destination zone.	–
Interface name	Name of the interface.	–
Bytes sent by this user	Number of packets in bytes sent by this user.	–
Bytes received by this user	Number of packets in bytes received by this user.	–
Client-groups	Name of the client group.	–

Table 119: Summary of Key Firewall Authentication History Output Fields *(continued)*

Field	Values	Additional Information
Detail history of selected Source Ip:*Source Ip*		
User	Name of the user.	–
Start Date	Authentication date.	–
Start Time	Authentication time.	–
Duration	Authentication duration.	–
Status	Status of authentication (**success** or **failure**).	–
Profile	Name of the profile.	–
Authentication method	Path chosen for authentication.	–
Policy Id	Security policy identifier.	–
Source zone	Name of the source zone.	–
Destination Zone	Name of the destination zone.	–
Interface name	Name of the interface.	–
Bytes sent by this user	Number of packets in bytes sent by this user.	–
Bytes received by this user	Number of packets in bytes received by this user.	–
Client-groups	Name of the client group.	–

Monitoring 802.1x

Purpose

View information about 802.1X properties.

Action

Select **Monitor>Security>802.1x** in the J-Web user interface, or enter the following CLI commands:

- **show dot1x interfaces *interface-name***
- **show dot1x authentication-failed-users**

Table 120 on page 1094 summarizes the Dot1X output fields.

Table 120: Summary of Dot1X Output Fields

Field	Values	Additional Information
Select Port	List of ports for selection.	–
Number of connected hosts	Total number of hosts connected to the port.	–
Number of authentication bypassed hosts	Total number of authentication-bypassed hosts with respect to the port.	–
Authenticated Users Summary		
MAC Address	MAC address of the connected host.	–
User Name	Name of the user.	–
Status	Information about the host connection status.	–
Authentication Due	Information about host authentication.	–
Authentication Failed Users Summary		
MAC Address	MAC address of the authentication-failed host.	–
User Name	Name of the authentication-failed user.	–

SEE ALSO

Monitoring Application Firewalls

RELATED DOCUMENTATION

Monitoring Overview | 15

Monitoring Interfaces | 1100

CHAPTER 31

Monitoring Interfaces and Switching Functions

IN THIS CHAPTER

- Displaying Real-Time Interface Information | 1096
- Monitoring Ethernet Switching | 1099
- Monitoring Interfaces | 1100
- Monitoring PPP | 1102

Displaying Real-Time Interface Information

Enter the **monitor interface** command to display real-time traffic, error, alarm, and filter statistics about a physical or logical interface:

```
user@host> monitor interface (interface-name | traffic)
```

Replace ***interface-name*** with the name of a physical or logical interface. If you specify the **traffic** option, statistics for all active interfaces display.

The real-time statistics update every second. The **Current delta** and **Delta** columns display the amount the statistics counters have changed since the **monitor interface** command was entered or since you cleared the delta counters. Table 121 on page 1096 and Table 122 on page 1097 list the keys you use to control the display using the ***interface-name*** and **traffic** options. (The keys are not case sensitive.)

Table 121: CLI monitor interface Output Control Keys

Key	Action
c	Clears (returns to 0) the delta counters in the **Current delta** column. The statistics counters are not cleared.
f	Freezes the display, halting the update of the statistics and delta counters.
i	Displays information about a different interface. You are prompted for the name of a specific interface.

Table 121: CLI monitor interface Output Control Keys *(continued)*

Key	Action
n	Displays information about the next interface. The device scrolls through the physical and logical interfaces in the same order in which they are displayed by the **show interfaces terse** command.
q or ESC	Quits the command and returns to the command prompt.
t	Thaws the display, resuming the update of the statistics and delta counters.

Table 122: CLI monitor interface traffic Output Control Keys

Key	Action
b	Displays the statistics in units of bytes and bytes per second (bps).
c	Clears (returns to 0) the delta counters in the **Delta** column. The statistics counters are not cleared.
d	Displays the **Delta** column instead of the rate column—in bps or packets per second (pps).
p	Displays the statistics in units of packets and packets per second (pps).
q or ESC	Quits the command and returns to the command prompt.
r	Displays the rate column—in bps and pps—instead of the **Delta** column.

The following are sample displays from the **monitor interface** command:

```
user@host> monitor interface fe-0/0/0
```

```
host1                          Seconds: 5                 Time: 04:38:40
                                                        Delay: 3/0/10
Interface: fe-0/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 1000mbps
Traffic statistics:                                        Current delta
  Input bytes:                885405423 (3248 bps)                [2631]
  Output bytes:               137411893 (3344 bps)               [10243]
```

```
  Input packets:                7155064 (2 pps)                     [28]
  Output packets:                636071 (1 pps)                     [23]
Error statistics:
  Input errors:                       0                             [0]
  Input drops:                        0                             [0]
  Input framing errors:               0                             [0]
  Policed discards:                   0                             [0]
  L3 incompletes:                     0                             [0]
  L2 channel errors:                  0                             [0]
  L2 mismatch timeouts:               0                             [0]
  Carrier transitions:                1                             [0]
  Output errors:                      0                             [0]
  Output drops:                       0                             [0]
  Aged packets:                       0                             [0]
Active alarms : None
Active defects: None
Input MAC/Filter statistics:
  Unicast packets                 73083                             [16]
  Broadcast packets             3629058                              [5]
  Multicast packets             3511364                              [3]
  Oversized frames                    0                             [0]
  Packet reject count                 0                             [0]
  DA rejects                          0                             [0]
  SA rejects                          0                             [0]
Output MAC/Filter Statistics:
  Unicast packets                629555                             [28]
  Broadcast packets                6494  Multicast packet            [0]
```

NOTE: The output fields that display when you enter the **monitor interface *interface-name*** command are determined by the interface you specify.

```
user@host> monitor interface traffic
```

```
Interface    Link  Input packets        (pps)     Output packets        (pps)
fe-0/0/0      Up          42334          (5)              23306          (3)
fe-0/0/1      Up      587525876      (12252)          589621478      (12891)
```

RELATED DOCUMENTATION

Monitoring Interfaces | 1100

Monitoring Ethernet Switching

Purpose

View information about the Ethernet Switching interface details.

Action

Select **Monitor>Switching>Ethernet Switching** in the J-Web user interface, or enter the following CLI commands:

- **show ethernet-switching table**
- **show ethernet-switching mac-learning-log**

Table 123 on page 1099 summarizes the Ethernet Switching output fields.

Table 123: Summary of Ethernet Switching Output Fields

Field	Values	Additional Information
VLAN	The VLAN for which Ethernet Switching is enabled.	-
MAC Address	The MAC address associated with the VLAN. If a VLAN range has been configured for a VLAN, the output displays the MAC addresses for the entire series of VLANs that were created with that name.	-
Type	The type of MAC address. Values are: • static—The MAC address is manually created. • learn—The MAC address is learned dynamically from a packet's source MAC address. • flood—The MAC address is unknown and flooded to all members.	-
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	-

Table 123: Summary of Ethernet Switching Output Fields *(continued)*

Field	Values	Additional Information
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).	-
VLAN-ID	The VLAN ID.	-
MAC Address	The learned MAC address.	-
Time	Timestamp when the MAC address was added or deleted from the log.	-
State	Indicates the MAC address learned on the interface.	-

RELATED DOCUMENTATION

Monitoring Overview | 15

Monitoring Interfaces | 1100

Monitoring Interfaces

Purpose

View general information about all physical and logical interfaces for a device.

Action

Enter the following **show** commands in the CLI to view interface status and traffic statistics.

- **show interfaces terse**

> **NOTE:** On SRX Series devices, when configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

- **show interfaces extensive**
- **show interfaces*interface-name***

NOTE: If you are using the J-Web user interfaces, select **Monitor>Interfaces** in the J-Web user interface. The J-Web Interfaces page displays the following details about each device interface:

- Port—Indicates the interface name.
- Admin Status—Indicates whether the interface is enabled (Up) or disabled (Down).
- Link Status—Indicates whether the interface is linked (Up) or not linked (Down).
- Address—Indicates the IP address of the interface.
- Zone—Indicates whether the zone is an untrust zone or a trust zone.
- Services—Indicates services that are enabled on the device, such as HTTP and SSH.
- Protocols—Indicates protocols that are enabled on the device, such as BGP and IGMP.
- Input Rate graph—Displays interface bandwidth utilization. Input rates are shown in bytes per second.
- Output Rate graph—Displays interface bandwidth utilization. Output rates are shown in bytes per second.
- Error Counters chart—Displays input and output error counters in the form of a bar chart.
- Packet Counters chart—Displays the number of broadcast, unicast, and multicast packet counters in the form of a pie chart. (Packet counter charts are supported only for interfaces that support MAC statistics.)

To change the interface display, use the following options:

- Port for FPC—Controls the member for which information is displayed.
- Start/Stop button—Starts or stops monitoring the selected interfaces.
- Show Graph—Displays input and output packet counters and error counters in the form of charts.
- Pop-up button—Displays the interface graphs in a separate pop-up window.
- Details—Displays extensive statistics about the selected interface, including its general status, traffic information, IP address, I/O errors, class-of-service data, and statistics.
- Refresh Interval—Indicates the duration of time after which you want the data on the page to be refreshed.
- Clear Statistics—Clears the statistics for the selected interface.

RELATED DOCUMENTATION

Interfaces User Guide for Security Devices

Monitoring PPP

Purpose

Display PPP monitoring information, including PPP address pool information, session status for PPP interfaces, cumulative statistics for all PPP interfaces, and a summary of PPP sessions.

> **NOTE:** PPP monitoring information is available only in the CLI. The J-Web user interface does not include pages for displaying PPP monitoring information.

Action

Enter the following CLI commands:

- **show ppp address-pool *pool-name***
- **show ppp interface *interface-name***
- **show ppp statistics**
- **show ppp summary**

RELATED DOCUMENTATION

Monitoring Overview | **15**

Monitoring Interfaces | **1100**

CHAPTER 32

Monitoring Events, Services and System

IN THIS CHAPTER

- Monitoring the System | 1103

Monitoring the System

IN THIS SECTION

- Monitoring System Properties for SRX Series Devices | 1103
- Monitoring Chassis Information | 1106
- System Health Management for SRX Series Devices | 1107

The J-Web user interface lets you monitor a device's physical characteristics, current processing status and alarms, and ongoing resource utilization to quickly assess the condition of a device at any time.

On SRX Series devices, the **Dashboard** lets you customize your view by selecting which informational panes to include on the Dashboard.

This section contains the following topics:

Monitoring System Properties for SRX Series Devices

Purpose

View system properties and customize the Dashboard.

When you start the J-Web user interface on an SRX Series device, the interface opens to the Dashboard. At the top and bottom of the page, the Dashboard displays an interactive representation of your device and a current log messages pane. By default, the center panes of the Dashboard display System Information, Resource Utilization, Security Resources, and System Alarms. However, you can customize the Dashboard panes to provide the best overview of your system.

Action

To control the content and appearance of the Dashboard:

1. Click the **Preferences** icon at the top-right corner of the page. The Dashboard Preference dialog box appears.

2. Select the types of information you want to display.

3. (Optional) Specify the Automatically Refresh Data option to specify how often you want the data on the Dashboard to be refreshed.

4. Click **OK** to save the configuration or **Cancel** to clear it.

5. On the Dashboard, minimize, maximize, or drag the individual information panes to customize the display as needed.

Chassis View—Displays an image of the device chassis, including line cards, link states, errors, individual PICs, FPCs, fans, and power supplies.

You can use the Chassis View to link to corresponding configuration and monitoring pages for the device. To link to interface configuration pages for a selected port from the Chassis View, right-click the port in the device image and choose one of the following options:

- Chassis Information—Links to the Chassis page.
- Configure Port: *Port-name*—Links to the interfaces configuration page for the selected port.
- Monitor Port: *Port-name*—Links to the monitor interfaces page for the selected port.

System Identification—Displays the device's serial number, hostname, current software version, the BIOS version, the amount of time since the device was last booted, and the system's time.

NOTE:

- To view the BIOS version under system identification, delete your browser cookies.
- The hostname that appears in this pane is defined using the **set system hostname** command.

  On SRX Series devices, security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs.

Resource Utilization—Provides a graphic representation of resource use. Each bar represents the percentage of CPU, memory, or storage utilization for the data plane or the control plane.

Security Resources—Provides the maximum, configured, and active sessions; firewall and VPN policies; and IPsec VPNs. Click **Sessions**,**FW/VPN Policies**, or **IPsec VPNs** for detailed statistics about each category.

System Alarms—Indicates a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified.

File Usage—Displays the usage statistics for log files, temporary files, crash (core) files, and database files.

Login Sessions—Provides a list of all currently logged in sessions. The display includes user credentials, login time, and idle time for each session.

Chassis Status—Provides a snapshot of the current physical condition of the device, including temperature and fan status.

Storage Usage—Displays the storage usage report in detail.

Threat Activity—Provides information about the most current threats received on the device.

Message Logs—Displays log messages and errors. You can clear old logs from the Message Logs pane by clicking the Clear button.

To control the information that is displayed in the Chassis View, use the following options:

- To view an image of the front of the device, right-click the image and choose **View Front**.
- To view an image of the back of the device, right-click the image and choose **View Rear**.
- To enlarge or shrink the device view, use the **Zoom** bar.
- To return the device image to its original position and size, click **Reset**.

> **NOTE:** To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View appears by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box. Clearing cookies in Internet Explorer also causes the Chassis View appear on the Dashboard page.

To return to the Dashboard at any time, select **Dashboard** in the J-Web user interface.

Alternatively, you can view system properties by entering the following **show** commands in the CLI:

- **show system uptime**
- **show system users**

- **show system storage**
- **show version**
- **show chassis hardware**

Monitoring Chassis Information

Purpose

View chassis properties, which include the status of hardware components on the device.

Action

To view these chassis properties, select **Monitor>System View>Chassis Information** in the J-Web user interface.

> **CAUTION:** Do not install a combination of Physical Interface Modules (PIMs) in a single chassis that exceeds the maximum power and heat capacity of the chassis. If power management is enabled, PIMs that exceed the maximum power and heat limits remain offline when the chassis is powered on. To check PIM power and heat status, use the **show chassis fpc** and **show chassis power-ratings** commands.

The Chassis Information page displays the following types of information:

- Routing Engine Details—This section of the page includes the following tabs:
  - Master—Master tab displays information about the routing engine, including the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.
  - Backup—If a backup routing engine is available, the Backup tab displays the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.

    > **NOTE:** If you need to contact customer support about the device chassis, supply them with the version and serial number displayed in the Routing Engine Details section of the page.

- Power and Fan Tray Details—This Details section of the page includes the following tabs:
  - Power—Power tab displays the names of the device's power supply units and their statuses.
  - Fan—Fan tab displays the names of the device's fans and their speeds (normal or high). (The fan speeds are adjusted automatically according to the current temperature.)
- Chassis Component Details—This section of the page includes the following tabs:

- General—General tab displays the version number, part number, serial number, and description of the selected device component.
- Temperature—Temperature tab displays the temperature of the selected device component (if applicable).
- Resource—Resource tab displays the state, total CPU DRAM, and start time of the selected device component (if applicable).

  NOTE: On some devices, you can have an FPC state as "offline." You might want to put an FPC offline because of an error or if the FPC is not responding. You can put the FPC offline by using the CLI command **request chassis fpc slot number offline**.

- Sub-Component—Sub-Component tab displays information about the device's sub-components (if applicable). Details include the sub-component's version, part number, serial number, and description.

To control which component details appear, select a hardware component from the **Select component** list.

Alternatively, you can view chassis details by entering the following **show** commands in the CLI configuration editor:

- **show chassis hardware**
- **show chassis routing-engine**
- **show chassis environment**
- **show chassis redundant-power-supply**
- **show redundant-power-supply status**

SEE ALSO

> *Monitoring Cluster Status*
>
> *Monitoring Cluster Statistics*

System Health Management for SRX Series Devices

Purpose

Tracking the utilization of critical resources in the system ensures that all parameters are within normal limits and the system remains functional.

In the event of a malfunction caused by abnormal resource usage, the system health management feature provides the right diagnostic information to identify the source of the problem.

When the system health management action is configured by the user, the system takes appropriate monitoring, preventive, and recovery actions to ensure that the system is accessible. The system configuration might be updated based on the information collected by system health management feature to ensure that the system stays in the normal operating environment. For example, when a system runs out of memory, then the configuration associated with applications identified to be consuming memory resources can be updated to bring down the memory resource consumption.

Action

The system health management feature periodically monitors critical system resources against configurable thresholds. The resources that can be monitored include CPU usage, memory, storage, open-file-descriptor, process-count, and temperature. The system health management feature collects usage information for each resource at the configured interval and compares it against the three levels of thresholds: moderate, high, and critical. Based on the configurations, appropriate action is taken.

The intervals, thresholds, and action are associated with system health management and can be configured at both the resource level and the global level. Configurable and default levels are as follows:

- Default configuration level— Default configuration is applied when system health monitoring is enabled, and neither a global nor a resource-specific configuration is present.
- Global configuration level—Configuration that is applied to resources when no resource-specific configuration is available.
- Resource-specific configuration level—Configuration that, if available, overrides both the global and the default configurations.

Per-resource configurations take precedence over the global configuration, and a global configuration takes precedence over the defaults.

When resource usage exceeds the configured thresholds, the system collects information that can be used to find the source of the increased usage and saves it in history for analysis and action.

When resource utilization exceeds the high threshold, a minor system alarm is generated, and the alarm LED lights yellow. When resource utilization exceeds the critical threshold, a major alarm is generated, and the alarm LED lights red.

An SNMP trap is also sent to the remote monitoring server (NMS) for all events that exceed the threshold.

To enable the system health monitor, use the **set snmp health-monitor routing engine** command. You can view system properties by using CLI show commands.

RELATED DOCUMENTATION

Monitoring Overview | 15

Monitoring Interfaces | 1100

CHAPTER 33

Monitoring Unified Threat Management Features

IN THIS CHAPTER

- Monitoring Reports | 1110

Monitoring Reports

IN THIS SECTION

- Threats Monitoring Report | 1110
- Traffic Monitoring Report | 1116

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action. The J-Web reporting feature provides one- or two-page reports that are equivalent to a compilation of numerous log entries.

This section contains the following topics:

Threats Monitoring Report

Purpose

Use the Threats Report to monitor general statistics and activity reports of current threats to the network. You can analyze logging data for threat type, source and destination details, and threat frequency information. The report calculates, displays, and refreshes the statistics, providing graphic presentations of the current state of the network.

Action

To view the Threats Report:

1. Click **Threats Report** in the bottom right of the Dashboard, or select **Monitor>Reports>Threats** in the J-Web user interface. The Threats Report appears.

2. Select one of the following tabs:
   - **Statistics** tab. See Table 124 on page 1111 for a description of the page content.
   - **Activities** tab. See Table 125 on page 1113 for a description of the page content.

Table 124: Statistics Tab Output in the Threats Report

Field	Description
General Statistics Pane	

Threat Category	One of the following categories of threats:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter—Click the Web filter category to display counters for 39 subcategories.
	  ◦ Content Filter
	• Firewall Event

Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Hits in past 24 hours	Number of threats encountered per category in the past 24 hours.
Hits in current hour	Number of threats encountered per category in the last hour.
Threat Counts in the Past 24 Hours	

Table 124: Statistics Tab Output in the Threats Report *(continued)*

Field	Description
By Severity	Graph representing the number of threats received each hour for the past 24 hours sorted by severity level.
By Category	Graph representing the number of threats received each hour for the past 24 hours sorted by category.
X Axis	Twenty-four hour span with the current hour occupying the right-most column of the display. The graph shifts to the left every hour.
Y Axis	Number of threats encountered. The axis automatically scales based on the number of threats encountered.
Most Recent Threats	
Threat Name	Names of the most recent threats. Depending on the threat category, you can click the threat name to go to a scan engine site for a threat description.

Category	Category of each threat:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter
	  ◦ Content Filter
	• Firewall Event

Source IP/Port	Source IP address (and port number, if applicable) of the threat.
Destination IP/Port	Destination IP address (and port number, if applicable) of the threat.
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail

Table 124: Statistics Tab Output in the Threats Report *(continued)*

Field	Description
Action	Action taken in response to the threat.
Hit Time	Time the threat occurred.
Threat Trend in past 24 hours	

Category	Pie chart graphic representing comparative threat counts by category:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter
	  ◦ Content Filter
	• Firewall Event

Web Filter Counters Summary	
Category	Web filter count broken down by up to 39 subcategories. Clicking on the Web filter listing in the General Statistics pane opens the Web Filter Counters Summary pane.
Hits in past 24 hours	Number of threats per subcategory in the last 24 hours.
Hits in current hour	Number of threats per subcategory in the last hour.

Table 125: Activities Tab Output in the Threats Report

Field	Function
Most Recent Virus Hits	
Threat Name	Name of the virus threat. Viruses can be based on services, like Web, FTP, or e-mail, or based on severity level.

Table 125: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Severity	Severity level of each threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP/Port	IP address (and port number, if applicable) of the source of the threat.
Destination IP/Port	IP address (and port number, if applicable) of the destination of the threat.
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail
Action	Action taken in response to the threat.
Last Hit Time	Last time the threat occurred.
Most Recent Spam E-Mail Senders	
From e-mail	E-mail address that was the source of the spam.

Table 125: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP	IP address of the source of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time that the spam e-mail was sent.
Recently Blocked URL Requests	
URL	URL request that was blocked.
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Hits in current hour	Number of threats encountered in the last hour.
Most Recent IDP Attacks	
Attack	

Table 125: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Severity	Severity of each threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Protocol	Protocol name of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time the IDP threat was sent.

SEE ALSO

Traffic Monitoring Report | **1116**

Monitoring Address Pools

Traffic Monitoring Report

Purpose

Monitor network traffic by reviewing reports of flow sessions over the past 24 hours. You can analyze logging data for connection statistics and session usage by a transport protocol.

Action

To view network traffic in the past 24 hours, select **Monitor>Reports>Traffic** in the J-Web user interface. See Table 126 on page 1117 for a description of the report.

Table 126: Traffic Report Output

Field	Description
Sessions in Past 24 Hours per Protocol	
Protocol Name	Name of the protocol. To see hourly activity by protocol, click the protocol name and review the “Protocol activities chart” in the lower pane. • TCP • UDP • ICMP
Total Session	Total number of sessions for the protocol in the past 24 hours.
Bytes In (KB)	Total number of incoming bytes in KB.
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Most Recently Closed Sessions	
Source IP/Port	Source IP address (and port number, if applicable) of the closed session.
Destination IP/Port	Destination IP address (and port number, if applicable) of the closed session.
Protocol	Protocol of the closed session. • TCP • UDP • ICMP
Bytes In (KB)	Total number of incoming bytes in KB.
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Timestamp	The time the session was closed.
Protocol Activities Chart	

Table 126: Traffic Report Output *(continued)*

Field	Description
Bytes In/Out	Graphic representation of traffic as incoming and outgoing bytes per hour. The byte count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
Packets In/Out	Graphic representation of traffic as incoming and outgoing packets per hour. The packet count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
Sessions	Graphic representation of traffic as the number of sessions per hour. The session count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
X Axis	One hour per column for 24 hours.
Y Axis	Byte, packet, or session count.
Protocol Session Chart	
Sessions by Protocol	Graphic representation of the traffic as the current session count per protocol. The protocols displayed are TCP, UDP, and ICMP.

SEE ALSO

Threats Monitoring Report | 1110

RELATED DOCUMENTATION

Monitoring Overview | 15

Monitoring Interfaces | 1100

PART 9

Performance Management

Configuring Network Analytics | **1120**

CHAPTER 34

Configuring Network Analytics

IN THIS CHAPTER

- Network Analytics Overview | 1120
- Understanding Enhanced Network Analytics Streaming Data | 1130
- Understanding Enhanced Analytics Local File Output | 1137
- Understanding Network Analytics Streaming Data | 1140
- Understanding Network Analytics Configuration and Status | 1143
- Prototype File for the Google Protocol Buffer Stream Format | 1144
- Configuring Queue Monitoring | 1145
- Configuring Traffic Monitoring | 1147
- Configuring a Local File for Network Analytics Data | 1149
- Configuring a Remote Collector for Streaming Analytics Data | 1150
- Example: Configuring Network Analytics | 1152
- Example: Configuring Enhanced Network Analytics Features | 1160

Network Analytics Overview

IN THIS SECTION

- Analytics Feature Overview | 1121
- Network Analytics Enhancements Overview | 1122
- Summary of CLI Changes | 1123

The network analytics feature provides you visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed. The analytics manager (analyticsm) in the Packet

Forwarding Engine collects traffic and queue statistics, and the analytics daemon (analyticsd) in the Routing Engine analyzes the data and generates reports. You can enable network analytics by configuring microburst monitoring and high-frequency traffic statistics monitoring.

> **NOTE:** In Junos OS Release 13.2X51-D15, the network analytics feature was enhanced, and extensive changes were made to the CLI statements and hierarchies. If you upgrade to Junos OS Release 13.2X51-D15 or later from a release prior to 13.2X51-D15, network analytics configurations committed in previous releases will appear on your device, but the feature is disabled. To enable this feature, you must reconfigure it using the new CLI statements and hierarchies.

For more information, see:

Analytics Feature Overview

You enable network analytics by configuring queue (microburst) monitoring and high-frequency traffic statistics monitoring. You use microburst monitoring to look at traffic queue conditions in the network. A microburst occurrence indicates to the Packet Forwarding Engine that a user-specified queue depth or latency threshold is reached. The queue depth is the buffer (in bytes) containing the data, and latency is the time (in nanoseconds or microseconds) the data stays in the queue.

You can configure queue monitoring based on either queue depth or latency (but not both), and configure the frequency (polling interval) at which the Packet Forwarding Engine checks for microbursts and sends the data to the Routing Engine for processing. You may configure queue monitoring globally for all physical interfaces on the system, or for a specific interface on the switch. However, the specified queue monitoring interval applies either to all interfaces, or none; you cannot configure the interval for each interface.

You use high-frequency traffic statistics monitoring to collect traffic statistics at specified polling intervals. Similar to the queue monitoring interval, the traffic monitoring interval applies either to all interfaces, or none; you cannot configure the interval for each interface.

Both traffic and queue monitoring are disabled by default. You must configure each type of monitoring using the CLI. In each case, the configuration for an interface always takes precedence over the global configuration.

> **NOTE:** You can configure traffic and queue monitoring for physical interfaces only; logical interfaces and Virtual Chassis port (VCP) interfaces are not supported.

The analyticsd daemon in the Routing Engine generates local log files containing queue and traffic statistics records. You can specify the log filename and size, and the number of log files. If you do not configure a filename, the data is not saved.

You can display the local log file or specify a server to receive the streaming data containing the queue and traffic statistics.

For each port, information for the last 10 records of traffic statistics and 100 records of queue statistics is cached. You may view this information by using the **show analytics** commands.

To store traceoptions data, you configure the **traceoptions** statement at the **[edit services analytics]** hierarchy level.

Network Analytics Enhancements Overview

Beginning in Junos OS Release 13.2X51-D15, the network analytics feature provides the following enhancements:

- Resources—Consist of interfaces and system. The interfaces resource allows you to configure an interface name and an associated resource profile name for each interface. With the system resource, you can configure the polling intervals for queue monitoring and traffic monitoring, and an associated resource profile for the system.
- Resource profile—A template that contains the configurations for queue and traffic monitoring, such as depth threshold and latency threshold values, and whether each type of monitoring is enabled or disabled. Once a resource profile is configured, you apply it to a system or interfaces resource.
- Collector—A server for collecting queue and traffic monitoring statistics, and can be a local or remote server. You can configure a local server to store monitoring statistics in a log file, or a remote server to receive streamed statistics data.
- Export profile—You must configure an export profile if you wish to send streaming data to a remote collector. In the export profile, you define the category of streamed data (system-wide or interface-specific) to determine stream type the collector will receive. You can specify both system and interface stream categories. System data includes system information and status of queue and traffic monitoring. Interface-specific data includes interface information, queue and traffic statistics, and link, queue, and traffic status.
- Google Protocol Buffer (GBP) stream format—A new streaming format for monitoring statistics data that is sent to a remote collector in a single AnRecord message. This stream format provides nine types of information, including:
  - System information—General system information, including boot time, model information, serial number, number of ports, and so on.
  - System queue status—Queue status for the system in general.
  - System traffic status—Traffic status for the system in general.

  - Interface information—Includes SNMP index, slot, port, and other information.
  - Queue statistics for interfaces—Queue statistics for specific interfaces.
  - Traffic statistics for interfaces—Traffic statistics for specific interfaces.
  - Link status for interfaces—Includes link speed, state, and so on.
  - Queue status for interfaces—Queue status for specific interfaces.
  - Traffic status for interfaces—Traffic status for specific interfaces.
- The **analytics.proto** file—Provides a template for the GBP stream format. This file can be used for writing your analytics server application. To download the file, go to:

  https://www.juniper.net/documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt
- Use of threshold values—The Analytics Manager (analyticsm) will generate a queue statistics record when the lower queue depth or latency threshold value is exceeded.
- User Datagram Protocol (UDP)—Additional transport protocol you can configure, in addition to Transmission Control Protocol (TCP), for the remote streaming server port.
- Single file for local logging—Replaces the separate log files for queue and traffic statistics.
- Change in latency measurement—Configuration and reporting of latency values have changed from microseconds to nanoseconds.
- Change in reporting of the collection time in UTC format—Statistics collection time is reported in microseconds instead of milliseconds.
- New operational mode command **show analytics collector**—Replaces the **show analytics streaming-server** command.
- Changes in command output format—Include the following changes:
  - Addition of unicast, multicast, and broadcast packet counters in queue and traffic statistics.
  - Reversal of the sequence of statistics information in the output. The most recent record is displayed at the beginning, and the oldest record at the end of the output.
  - Removal of traffic or queue monitoring status information from the global portion of the **show analytics configuration** and **show analytics status** command output if there is no global configuration.
  - Addition of **n/a** to the interface-specific portion of the **show analytics configuration** and **show analytics status** command output if a parameter is not configured (for example, depth threshold or latency threshold).

Summary of CLI Changes

Beginning in Junos OS Release 13.2X51-D15, enhancements to the network analytics feature result in changes in the CLI when you configure the feature. See Table 127 on page 1124 for a summary of CLI changes.

Table 127: Network Analytics CLI Changes

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring global queue and traffic monitoring polling interval	**[edit services analytics]**
	traffic-statistics {
	interval *interval*;
	}
	queue-statistics {
	interval *interval*;
	}
		[edit services analytics]
		resource {
		system {
		polling-interval {
		queue-monitoring *interval*;
		traffic-monitoring *interval*;
		}
		}
		}

Configuring local files for traffic and queue statistics reporting	**[edit services analytics]**
	traffic-statistics {
	file *filename*;
	size *size*;
	files *number*;
	}
	queue-statistics {
	file *filename*;
	size *size*;
	files *number*;
	}
		[edit services analytics]
		collector {
		local {
		file *filename* {
		files *number*;
		size *size*;
		}
		}
		}

Table 127: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Enabling queue statistics and traffic monitoring, and specifying the depth threshold for all interfaces (globally)	**[edit services analytics]**
	interfaces {
	all {
	queue-statistics;
	traffic-statistics;
	depth-threshold {
	high *number*;
	low *number*;
	}
	}
	}
		Requires defining a resource profile and applying it to the system:
		1. To define a resource profile:
		[edit services analytics]
		resource-profiles {
		profile-name{
		queue-monitoring;
		traffic-monitoring;
		depth-threshold {
		high *number*;
		low *number*;
		}
		}
		}
		2. To apply a profile to the system:
		[edit services analytics]
		resource {
		system {
		resource-profile *profile-name*;
		}
		}

Table 127: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Enabling queue statistics and traffic monitoring, and specifying the latency threshold for one interface	**[edit services analytics]**
	interfaces {
	interface{
	queue-statistics;
	traffic-statistics;
	latency-threshold
	high *number*;
	low *number*;
	}
	}
		Requires defining a resource profile and applying it to the interface:
		1. To define a resource profile:
		[edit services analytics]
		resource-profiles {
		profile-name{
		queue-monitoring;
		traffic-monitoring;
		latency-threshold {
		high *number*;
		low *number*;
		}
		}
		}
		2. To apply a profile to the interface:
		[edit services analytics]
		resource {
		interfaces {
		interface-name {
		resource-profile *profile-name*;
		}
		}
		}

Table 127: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring the streaming data format (JSON, CSV, or TSV) to send to a remote server
 	
NOTE: Junos OS Release 13.2X51-D15 added support for the GPB stream format and configuration of the transport protocols (TCP or UDP).
	[edit services analytics]
	
	streaming-servers {
	address *ip-address* {
	port *number* {
	stream-format *format*;
	}
	}
	}
		Requires defining the stream format in an export profile and applying the profile to the collector.
		
		1. To configure the stream format:
		
		[edit services analytics]
		
		export-profiles {
		profile-name {
		stream-format *format*;
		}
		}
		
		2. To apply an export profile to the collector:
		
		[edit services analytics]
		
		collector {
		address *ip-address* {
		port *number* {
		transport *protocol* {
		export-profile *profile-name*;
		}
		}
		}
		}

Table 127: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring the streaming message types (queue or traffic statistics) to send to a remote server	**[edit services analytics]**
	streaming-servers {
	address *ip-address* {
	port *number* {
	stream-type *type*;
	stream-type *type*;
	}
	}
	}
		Requires defining an export profile and applying it to the collector:
		1. To define an export profile:
		[edit services analytics]
		export-profiles {
		profile-name {
		interface {
		information;
		statistics {
		queue;
		traffic;
		}
		status {
		link;
		queue;
		traffic;
		}
		}
		system {
		information;
		status {
		queue;
		traffic;
		}
		}
		}
		}
		2. To apply an export profile to the collector:
		[edit services analytics]
		collector {
		address *ip-address* {
		port *number* {
		export-profile *profile-name*;
		}
		}
		}

Table 127: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring the transport protocol for sending streaming data to an external server	No configuration is available. Only the TCP protocol is supported.	Configuration is available. Both TCP and UDP protocols are supported, and can be configured for the same port.
		[edit services analytics]
		collector {
		address *ip-address* {
		port *number1* {
		transport tcp;
		transport udp;
		}
		port *number2* {
		transport udp;
		}
		}
		}

Show information about remote streaming server or collector	Issue the **show analytics streaming-sever** command.	Issue the **show analytics collector** command.

Release History Table

Release	Description
13.2X51-D15	In Junos OS Release 13.2X51-D15, the network analytics feature was enhanced, and extensive changes were made to the CLI statements and hierarchies.
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, the network analytics feature provides the following enhancements:
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, enhancements to the network analytics feature result in changes in the CLI when you configure the feature.

Understanding Enhanced Network Analytics Streaming Data

IN THIS SECTION

- Google Protocol Buffer (GPB) | 1130
- JavaScript Object Notation (JSON) | 1133
- Comma-separated Values (CSV) | 1134
- Tab-separated Values (TSV) | 1134
- Queue Statistics Output for JSON, CSV, and TSV | 1135
- Traffic Statistics Output for JSON, CSV, and TSV | 1135

Network analytics monitoring data can be streamed to remote servers called collectors. You can configure one or more collectors to receive streamed data containing queue and traffic statistics. This topic describes the streamed data output.

NOTE: This topic applies to Junos OS Release 13.2X51-D15 or later.

Starting in Junos OS Release 13.2X51-D15, network analytics supports the following streaming data formats and output:

Google Protocol Buffer (GPB)

Support for the Google Protocol Buffer (GPB) streaming format has been added in Junos OS Release 13.2X51-D15. This streaming format provides:

- Support for nine types of messages, based on resource type (system-wide or interface-specific).
- Sends messages in a hierarchical format.
- You can generate other stream format messages (JSON, CSV, TSV) from GPB formatted messages.
- Includes a 8-byte message header. See Table 128 on page 1131 for more information.

Table 128 on page 1131 describes the GPB stream format message header.

Table 128: GPB Stream Format Message Header Information

Byte Position	Field
0 to 3	Length of message
4	Message version
5 to 7	Reserved for future use

The following GPB prototype file (**analytics.proto**) provides details about the streamed data:

```
package analytics;

// Traffic statistics related info
message TrafficStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
}

// Queue statistics related info
message QueueStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
    optional uint64             lt_high         = 3;
    optional uint64             lt_low          = 4;
    optional uint64             dt_high         = 5;
    optional uint64             dt_low          = 6;
}

message LinkStatus {
    optional uint64             speed           = 1;
    optional uint32             duplex          = 2;
    optional uint32             mtu             = 3;
    optional bool               state           = 4;
    optional bool               auto_negotiation= 5;
}

message InterfaceInfo {
    optional uint32             snmp_index      = 1;
    optional uint32             index           = 2;
    optional uint32             slot            = 3;
    optional uint32             port            = 4;
    optional uint32             media_type      = 5;
```

```
    optional uint32             capability      = 6;
    optional uint32             porttype        = 7;
}

message InterfaceStatus {
    optional LinkStatus         link            = 1;
    optional QueueStatus        queue_status    = 2;
    optional TrafficStatus      traffic_status  = 3;
}

message QueueStats {
    optional uint64             timestamp       = 1;
    optional uint64             queue_depth     = 2;
    optional uint64             latency         = 3;
}

message TrafficStats {
    optional uint64             timestamp       = 1;
    optional uint64             rxpkt           = 2;
    optional uint64             rxucpkt         = 3;
    optional uint64             rxmcpkt         = 4;
    optional uint64             rxbcpkt         = 5;
    optional uint64             rxpps           = 6;
    optional uint64             rxbyte          = 7;
    optional uint64             rxbps           = 8;
    optional uint64             rxcrcerr        = 9;
    optional uint64             rxdroppkt       = 10;
    optional uint64             txpkt           = 11;
    optional uint64             txucpkt         = 12;
    optional uint64             txmcpkt         = 13;
    optional uint64             txbcpkt         = 14;
    optional uint64             txpps           = 15;
    optional uint64             txbyte          = 16;
    optional uint64             txbps           = 17;
    optional uint64             txcrcerr        = 18;
    optional uint64             txdroppkt       = 19;
}

message InterfaceStats {
    optional TrafficStats       traffic_stats   = 1;
    optional QueueStats         queue_stats     = 2;
}

//Interface message
```

```
message Interface {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional InterfaceInfo      information     = 3;
    optional InterfaceStats     stats           = 4;
    optional InterfaceStatus    status          = 5;
}

message SystemInfo {
    optional uint64             boot_time       = 1;
    optional string             model_info      = 2;
    optional string             serial_no       = 3;
    optional uint32             max_ports       = 4;
    optional string             collector       = 5;
    repeated string             interface_list  = 6;
}

message SystemStatus {
    optional QueueStatus        queue_status    = 1;
    optional TrafficStatus      traffic_status  = 2;
}

//System message
message System {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional SystemInfo         information     = 3;
    optional SystemStatus       status          = 4;
}

message AnRecord {
    optional uint64             timestamp       = 1;
    optional System             system          = 2;
    repeated Interface          interface       = 3;
}
```

JavaScript Object Notation (JSON)

The JavaScript Object Notation (JSON) streaming format supports the following data:

- Queue statistics data. For example:

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

See Table 129 on page 1135 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
{"record-type":"traffic-stats","time":1383453986763,"router-id":"qfx5100-switch",
"port":"xe-0/0/16","rxpkt":26524223621,"rxpps":8399588,"rxbyte":3395100629632,
"rxbps":423997832,"rxdrop":0,"rxerr":0,"txpkt":795746503,"txpps":0,"txbyte":101855533467,
"txbps":0,"txdrop":0,"txerr":0}
```

See Table 130 on page 1136 for more information about traffic statistics output fields.

Comma-separated Values (CSV)

The Comma-separated Values (CSV) streaming format supports the following data:

- Queue statistics. For example:

```
q,1383454067604,qfx5100-switch,xe-0/0/18,0,208
```

See Table 129 on page 1135 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
t,1383454072924,qfx5100-switch,xe-0/0/19,1274299748,82950,163110341556,85603312,0,0,
27254178291,8300088,3488534810679,600002408,27268587050,3490379142400
```

See Table 130 on page 1136 for more information about traffic statistics output fields.

Tab-separated Values (TSV)

The Tab-separated Values (TSV) streaming format supports the following data:

- Queue statistics. For example:

```
q       585870192561703872      qfx5100-switch       xe-0/0/18       (null)
208     2
```

See Table 129 on page 1135 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
t       1383454139025   qfx5100-switch  xe-0/0/19       1279874033      82022
163823850036    84801488        0       0       27811618258     8199630
3559887126455   919998736       27827356915     3561901685120
```

See Table 130 on page 1136 for more information about traffic statistics output fields.

Queue Statistics Output for JSON, CSV, and TSV

Table 129 on page 1135 describes the output fields for streamed queue statistics data in the order they appear.

Table 129: Streamed Queue Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **queue-stats** (JSON format) • **q** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
latency	Traffic queue latency in milliseconds.
queue depth	Depth of the traffic queue in bytes.

Traffic Statistics Output for JSON, CSV, and TSV

Table 130 on page 1136 describes the output fields for streamed traffic statistics data in the order they appear.

Table 130: Streamed Traffic Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **traffic-stats** (JSON format) • **t** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
rxpkt	Total packets received.
rxpps	Total packets received per second.
rxbyte	Total bytes received.
rxbps	Total bytes received per second.
rxdrop	Total incoming packets dropped.
rxerr	Total packets with errors.
txpkt	Total packets transmitted.
txpps	Total packets transmitted per second.
txbyte	Total bytes transmitted.
txbps	Total bytes transmitted per second.
txdrop	Total transmitted bytes dropped.
txerr	Total transmitted packets with errors (dropped).

Release History Table

Release	Description
13.2X51-D15	Starting in Junos OS Release 13.2X51-D15, network analytics supports the following streaming data formats and output:

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Prototype File for the Google Protocol Buffer Stream Format | 1144

collector (Analytics) | 2072

Understanding Enhanced Analytics Local File Output

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. You enable network analytics by configuring queue or traffic statistics monitoring, or both. In addition, you can configure a local file for storing the traffic and queue statistics records.

NOTE: This topic describes the local file output in Junos OS Release 13.2X51-D15 and later.

Beginning in Junos OS Release 13.2X51-D15, the traffic and queue monitoring statistics can be stored locally in a single file. The following example shows the output from the **monitor start** command.

root@qfx5100-33> monitor start an

```
root@qfx5100-33>
*** an ***
q,1393947567698432,qfx5100-33,xe-0/0/19,1098572,1373216
q,1393947568702418,qfx5100-33,xe-0/0/19,1094912,1368640
q,1393947569703415,qfx5100-33,xe-0/0/19,1103065,1378832
t,1393947569874528,qfx5100-33,xe-0/0/16,12603371884,12603371884,0,0,
8426023,1613231610488,8628248712,0,3,5916761,5916761,0,0,0,757345408,0,0,0
t,1393947569874528,qfx5100-33,xe-0/0/18,12601953614,12601953614,0,0,
8446737,1613050071660,8649421552,0,5,131761619,131761619,0,0,84468,
16865487232,86495888,0,0
t,1393947569874528,qfx5100-33,xe-0/0/19,126009250,126009250,0,0,84469,
16129184128,86496392,0,0,12584980342,12584980342,0,0,8446866,1610877487744,
8649588432,12593703960,0
q,1393947575698402,qfx5100-33,xe-0/0/19,1102233,1377792
q,1393947576701398,qfx5100-33,xe-0/0/19,1107724,1384656
```

See Table 131 on page 1138 for queue statistics output, and Table 132 on page 1138 for traffic statistics output. The fields in the tables are listed in the order they appear in the output example.

Table 131: Output Fields for Queue Statistics in Local Analytics File

Field	Description	Example in Output
Record type	Type of statistics (queue or traffic monitoring)	**q**
Time (microseconds)	Unix epoch (or Unix time) in microseconds at which the statistics were captured.	**1393947567698432**
Router ID	ID of the network analytics host device.	**qfx5100-33**
Port	Name of the physical port configured for network analytics.	**xe-0/0/19**
Latency (nanoseconds)	Traffic queue latency in nanoseconds.	**1098572**
Queue depth (bytes)	Depth of the traffic queue in bytes.	**1373216**

Table 132: Output Fields for Traffic Statistics in Local Analytics File

Field	Description	Example in Output
Record type	Type of statistics (queue or traffic monitoring)	**t**
Time (microseconds)	Unix epoch (or Unix time) in microseconds at which the statistics were captured.	**1393947569874528**
Router ID	ID of the network analytics host device.	**qfx5100-33**
Port	Name of the physical port configured for network analytics.	**xe-0/0/16**
rxpkt	Total packets received.	**12603371884**
rxucpkt	Total unicast packets received.	**12603371884**
rxmcpkt	Total multicast packets received.	**0**
rxbcpkt	Total broadcast packets received.	**0**
rxpps	Total packets received per second.	**8426023**
rxbyte	Total octets received.	**1613231610488**
rxbps	Total bytes received per second.	**8628248712**

Table 132: Output Fields for Traffic Statistics in Local Analytics File *(continued)*

Field	Description	Example in Output
rxdroppkt	Total incoming packets dropped.	**0**
rxcrcerr	CRC/Align errors received.	**3**
txpkt	Total packets transmitted.	**5916761**
txucpkt	Total unicast packets transmitted.	**5916761**
txmcpkt	Total multicast packets transmitted.	**0**
txbcpkt	Total broadcast packets transmitted.	**0**
txpps	Total packets transmitted per second.	**0**
txbyte	Total octets transmitted.	**757345408**
txbps	Bytes per second transmitted.	**0**
txdroppkt	Total transmitted packets dropped.	**0**
txcrcerr	CRC/Align errors transmitted.	**0**

Release History Table

Release	Description
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, the traffic and queue monitoring statistics can be stored locally in a single file.

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

Understanding Network Analytics Streaming Data

This topic describes the network analytics queue and traffic statistics that are streamed to remote servers.

You can configure one or more remote servers to receive streamed data containing queue and traffic statistics. The format of the streamed data can be Javascript Object Notation (JSON), Comma-separated Values (CSV), or Tab-separated Values (TSV).

> **NOTE:** The output shown in this topic applies to Junos OS Release 13.2X51-D10 only. The time is displayed in the Unix epoch format (also known as Unix time or POSIX time).

The following examples show the streamed queue statistics data output in different formats.

- JSON format:

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

- CSV format:

```
q,1383454067604,qfx5100-switch,xe-0/0/18,0,208
```

- TSV format:

```
q       585870192561703872      qfx5100-switch       xe-0/0/18       (null)
208     2
```

Table 129 on page 1135 describes the output fields for streamed queue statistics data in the order they appear.

Table 133: Streamed Queue Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **queue-stats** (JSON format) • **q** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.

Table 133: Streamed Queue Statistics Data Output Fields *(continued)*

Field	Description
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
latency	Traffic queue latency in milliseconds.
queue depth	Depth of the traffic queue in bytes.

The following examples show the streamed traffic statistics data output in different formats.

- JSON format:

```
{"record-type":"traffic-stats","time":1383453986763,"router-id":"qfx5100-switch",
"port":"xe-0/0/16","rxpkt":26524223621,"rxpps":8399588,"rxbyte":3395100629632,
"rxbps":423997832,"rxdrop":0,"rxerr":0,"txpkt":795746503,"txpps":0,"txbyte":101855533467,
"txbps":0,"txdrop":0,"txerr":0}
```

- CSV format:

```
t,1383454072924,qfx5100-switch,xe-0/0/19,1274299748,82950,163110341556,85603312,0,0,
27254178291,8300088,3488534810679,600002408,27268587050,3490379142400
```

- TSV format:

```
t       1383454139025   qfx5100-switch  xe-0/0/19       1279874033      82022
163823850036    84801488        0       0       27811618258     8199630
3559887126455   919998736       27827356915     3561901685120
```

Table 130 on page 1136 describes the output fields for streamed traffic statistics data in the order they appear.

Table 134: Streamed Traffic Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **traffic-stats** (JSON format) • **t** (CSV or TSV format)

Table 134: Streamed Traffic Statistics Data Output Fields *(continued)*

Field	Description
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
rxpkt	Total packets received.
rxpps	Total packets received per second.
rxbyte	Total bytes received.
rxbps	Total bits received per second.
rxdrop	Total incoming packets dropped.
rxerr	Total packets with errors.
txpkt	Total packets transmitted.
txpps	Total packets transmitted per second.
txbyte	Total bytes transmitted.
txbps	Total bytes transmitted per second.
txdrop	Total transmitted bytes dropped.
txerr	Total transmitted packets with errors (dropped).

RELATED DOCUMENTATION

Network Analytics Overview | 1120

streaming-servers | 2107

Understanding Network Analytics Configuration and Status

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. You can enable network analytics by configuring traffic and queue statistics monitoring.

> **NOTE:** This topic describes the configuration and status output from Junos OS Release 13.2X50-D15 and 13.2X51-D10 only.

If you had enabled traffic or queue monitoring, you can issue the **show analytics configuration** and **show analytics status** commands to view the global interface configuration and status and that of specific interfaces. The output that is displayed depends on your configuration at the global interface and specific interface levels. For example:

- A global interface configuration (for all interfaces) to disable monitoring supersedes the configuration to enable it on an interface.
- The interface configuration to enable or disable monitoring supersedes the global interface configuration, unless monitoring had been disabled globally for all interfaces.
- If there is no configuration, whether for all interfaces or a specific interface, monitoring is disabled by default (see Table 135 on page 1143).

Table 135 on page 1143 describes the correlation between the user configuration and the settings that are displayed.

Table 135: Configuration and Status Output in Junos OS Release 13.2X51-D10 and 13.2X50-D15

	Global or System Settings		Specific Interface Settings	
User Configuration	Configuration	Status	Configuration	Status
No global or specific interface configuration. This is the default setting.	Auto	Auto	Auto	Disabled
No global interface configuration but the specific interface monitoring is disabled.	Auto	Auto	Disabled	Disabled
No global interface configuration but the specific interface monitoring is enabled.	Auto	Auto	Enabled	Enabled
Monitoring is disabled globally and there is no interface configuration.	Disabled	Disabled	Auto	Disabled

Table 135: Configuration and Status Output in Junos OS Release 13.2X51-D10 and 13.2X50-D15 *(continued)*

User Configuration	Global or System Settings		Specific Interface Settings	
	Configuration	Status	Configuration	Status
Monitoring is disabled at both the global and specific interface levels.	Disabled	Disabled	Disabled	Disabled
Monitoring is disabled at the global interface level but is enabled at the specific interface level. The global interface *Disabled* setting supersedes the *Enabled* setting for a specific interface.	Disabled	Disabled	Enabled	Disabled
Monitoring is enabled for all interfaces but there is no configuration for the specific interface .	Enabled	Enabled	Auto	Enabled
Monitoring is enabled at both the global and specific interface levels.	Enabled	Enabled	Enabled	Enabled
Monitoring is enabled for all interfaces but is disabled for the specific interface.	Enabled	Enabled	Disabled	Disabled

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

queue-statistics | **2099**

traffic-statistics | **2116**

Prototype File for the Google Protocol Buffer Stream Format

The Google Protocol Buffer (GBP) stream format is used for streaming monitoring statistics data to a remote collector in a single AnRecord message.

The **analytics.proto** file provides a template for the GBP stream format. This file can be used for writing your analytics server application.

To download the GPB prototype file, go to:

https://www.juniper.net/documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt

RELATED DOCUMENTATION

Network Analytics Overview | 1120

export-profiles | 2076

Configuring Queue Monitoring

Network analytics queue monitoring provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. You can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You enable queue monitoring by first defining a resource profile template, and then applying the profile to the system (for a global configuration) or to individual interfaces.

NOTE: You can configure queue monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: The procedure to configure queue monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure queue monitoring on a QFX Series standalone switch:

1. Configure the queue monitoring polling interval (in milliseconds) globally (for the system):

   ```
   [edit]
   set services analytics resource system polling-interval queue-monitoring interval
   ```

2. Configure a resource profile for the system, and enable queue monitoring:

   ```
   [edit]
   set services analytics resource-profiles profile-name queue-monitoring
   ```

3. Configure high and low values of the depth-threshold (in bytes) for queue monitoring in the system profile:

   ```
   [edit]
   set services analytics resource-profiles profile-name depth-threshold high number low number
   ```

   For both high and low values, the range is from 1 to 1,250,000,000 bytes, and the default value is 0 bytes.

   NOTE: You can configure either the depth-threshold or latency threshold for the system, but not both.

4. Apply the resource profile template to the system for a global configuration:

   ```
   [edit]
   set services analytics resource system resource-profile profile-name
   ```

5. Configure an interface-specific resource profile and enable queue monitoring for the interface:

   ```
   [edit]
   set services analytics resource-profiles profile-name queue-monitoring
   ```

6. Configure the latency-threshold (high and low values) for queue monitoring in the interface-specific profile:

   ```
   [edit]
   set services analytics resource-profiles profile-name latency-threshold high number low number
   ```

   For both high and low values, the range is from 1 to 100,000,000 nanoseconds, and the default value is 1,000,000 nanoseconds.

   NOTE: You can configure either the depth-threshold or latency threshold for interfaces, but not both.

7. Apply the resource profile template for interfaces to one or more interfaces:

```
[edit]
set services analytics resource interfaces interface-name resource-profile profile-name
```

NOTE: If a conflict arises between the system and interface configurations, the interface-specific configuration supersedes the global (system) configuration.

Release History Table

Release	Description
13.2X51-D15	The procedure to configure queue monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Configuring Traffic Monitoring

Network analytics queue monitoring provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. You can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You enable traffic monitoring by first defining a resource profile template, and then applying the profile to the system (for a global configuration) or to individual interfaces.

NOTE: You can configure traffic monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: The procedure to configure traffic monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure traffic monitoring on a QFX Series standalone switch:

1. Configure the traffic monitoring polling interval (in seconds) for the system:

   ```
   [edit]
   set services analytics resource system polling-interval traffic-monitoring interval
   ```

2. Configure a resource profile for the system, and enable traffic monitoring in the profile:

   ```
   [edit]
   set services analytics resource-profiles profile-name traffic-monitoring
   ```

3. Apply the resource profile to the system for a global configuration:

   ```
   [edit]
   set services analytics resource system resource-profile profile-name
   ```

4. Configure a resource profile for interfaces, and enable traffic monitoring in the profile:

   ```
   [edit]
   set services analytics resource-profiles profile-name traffic-monitoring
   ```

   NOTE: If a conflict arises between the system and interface configurations, the interface-specific configuration supersedes the global (system) configuration.

5. Apply the resource profile template to one or more interfaces:

   ```
   [edit]
   set services analytics resource interfaces interface-name resource-profile profile-name
   ```

Release History Table

Release	Description
13.2X51-D15	The procedure to configure traffic monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Configuring a Local File for Network Analytics Data

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

To save the queue and traffic statistics data in a local file, you must configure a filename to store it.

> **NOTE:** The procedure to configure a local file for storing queue and traffic monitoring statistics requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure a local file for storing queue and traffic monitoring statistics:

1. Configure a filename:

   ```
   [edit]
   set services analytics collector local file filename
   ```

   There is no default filename. If you do not configure a filename, network analytics statistics are not saved locally.

2. Configure the number of files (from 2 to 1000 files):

   ```
   [edit]
   set services analytics collector local file filename files number
   ```

3. Configure the file size (from 10 to 4095 MB) in the format of xm:

   ```
   [edit]
   set services analytics collector local file an size size
   ```

Release History Table

Release	Description
13.2X51-D15	The procedure to configure a local file for storing queue and traffic monitoring statistics requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Configuring a Remote Collector for Streaming Analytics Data

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You can configure an export profile to define the stream format and type of data, and one or more remote servers (collectors) to receive streaming network analytics data.

> **NOTE:** The procedure to configure a collector for receiving streamed analytics data requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure a collector for receiving streamed analytics data:

1. Create an export profile and specify the stream format:

   ```
   [edit]
   set services analytics export-profiles profile-name stream-format format
   ```

2. Configure the export profile to include interface information:

   ```
   [edit]
   set services analytics export-profiles profile-name interface information
   ```

3. Configure the export profile to include interface queue statistics:

```
[edit]
set services analytics export-profiles profile-name interface statistics queue
```

4. Configure the export profile to include interface traffic statistics:

```
[edit]
set services analytics export-profiles profile-name interface statistics traffic
```

5. Configure the export profile to include interface status link information:

```
[edit]
set services analytics export-profiles profile-name interface status link
```

6. Configure the export profile to include system information:

```
[edit]
set services analytics export-profiles profile-name system information
```

7. Configure the export profile to include system queue status:

```
[edit]
set services analytics export-profiles profile-name system status queue
```

8. Configure the export profile to include system traffic status:

```
[edit]
set services analytics export-profiles profile-name system status traffic
```

9. Configure the transport protocol for the collector addresses and apply the export profile:

```
[edit]
set services analytics collector address ip-address port port transport protocol export-profile profile-name
set services analytics collector address ip-address port port transport protocol export-profile profile-name
```

NOTE: If you configure the **tcp** or **udp** option for the JSON, CSV, and TSV formats, you must also set up the TCP or UDP client software on the remote collector to process records that are separated by the newline character (\n) on the remote server.

If you configure the **tcp** or **udp** option for the GPB format, you must also set up the TCP or UDP build streaming server using the **analytics.proto** file.

Release History Table

Release	Description
13.2X51-D15	The procedure to configure a collector for receiving streamed analytics data requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Example: Configuring Network Analytics

IN THIS SECTION

- Requirements | 1153
- Overview | 1153
- Configuration | 1153
- Verification | 1157

This example shows how to configure network analytics which includes queue and traffic monitoring on a QFX3500 standalone switch.

NOTE: The configuration shown in this example is supported only on Junos OS Release 13.2X50-D15 and 13.2X51-D10.

Requirements

This example uses the following hardware and software components:

- A QFX3500 standalone switch
- A external streaming server to collect data
- Junos OS Release 13.2X50-D15 software
- TCP server software (for remote streaming servers)

Before you configure network analytics, be sure you have:

- Junos OS Release 13.2X50-D15 or later software installed and running on the QFX3500 switch
- (Optional for streaming servers) TCP server software set up for processing records separated by a newline character (\n) on the remote streaming server
- All other devices running

Overview

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed. You can enable network analytics by configuring queue and traffic statistics monitoring.

Topology

In this example, the QFX3500 switch is connected to an external server used for streaming statistics data.

Configuration

IN THIS SECTION

- Configuring Queue and Traffic Statistics Monitoring | **1154**
- Configuring Local Statistics Files | **1155**

Configuring Streaming Servers | 1155
Results | 1156

To configure network analytics, perform these tasks:

CLI Quick Configuration

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

```
[edit]
set services analytics interfaces all queue-statistics
set services analytics interfaces all latency-threshold high 900 low 300
set services analytics interfaces xe-0/0/1 traffic-statistics
set services analytics queue-statistics file qstats1.qs files 3 size 10
set services analytics queue-statistics interval 10
set services analytics traffic-statistics file tstats1.ts files 3 size 10
set services analytics traffic-statistics interval 2
set services analytics streaming-servers address 10.94.198.11 port 50001 stream-format json stream-type
    queue-statistics
set services analytics streaming-servers address 10.94.198.11 port 50005 stream-format csv stream-type
    traffic-statistics
```

Configuring Queue and Traffic Statistics Monitoring

Step-by-Step Procedure

To configure queue and traffic monitoring on physical interfaces:

NOTE: You can configure queue and traffic monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: Disabling of the queue or traffic monitoring supersedes the configuration (enabling) of this feature. You disable monitoring by issuing the **no-queue-statistics** or **no-traffic-statistics** at the **[edit services analytics interfaces]** hierarchy level.

1. Configure all interfaces for queue monitoring and set the latency thresholds (in microseconds):

```
[edit]
set services analytics interfaces all queue-statistics
set services analytics interfaces all latency-threshold high 900 low 300
```

2. Configure one interface for traffic monitoring:

```
[edit]
set services analytics interfaces xe-0/0/1 traffic-statistics
```

Configuring Local Statistics Files

Step-by-Step Procedure

To configure local statistics files:

1. Configure the number of queue statistics files, and each file size in MB:

```
[edit]
set services analytics queue-statistics file qstats1.qs files 3 size 10m
```

2. Configure the queue statistics collection interval in milliseconds

```
[edit]
set services analytics queue-statistics interval 10
```

3. Configure the number of traffic statistics files, and each file size in MB:

```
[edit]
set services analytics traffic-statistics file tstats1.ts files 3 size 10m
```

4. Configure the traffic statistics collection interval in seconds:

```
[edit]
set services analytics traffic-statistics interval 2
```

Configuring Streaming Servers

Step-by-Step Procedure

To configure streaming servers for receiving monitoring data:

> **NOTE:** In addition to configuring streaming servers, you must also set up the TCP client software to process records that are separated by the newline character (\n) on the remote server.

1. Configure a server IP address and port for queue statistics monitoring:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50001 stream-format json stream-type
    queue-statistics
```

2. Configure a server IP address and port for traffic statistics monitoring:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50005 stream-format csv stream-type
    traffic-statistics
```

Results

Display the results of the configuration:

```
[edit services analytics]
user@switch> show configuration
    queue-statistics {
        file qstats1.qs size 10m files 3;
        interval 10;
    }
    traffic-statistics {
        file tstats1.ts size 10m files 3;
        interval 2;
    }
    interfaces {
        xe-0/0/1 {
            traffic-statistics;
        }
        all {
            queue-statistics;
            latency-threshold high 900 low 300;
        }
    }
```

Verification

IN THIS SECTION

- Verifying the Network Analytics Configuration | 1157
- Verifying the Network Analytics Status | 1157
- Verifying Streaming Servers Configuration | 1158
- Verifying Queue Statistics | 1158
- Verifying Traffic Statistics | 1159

Confirm that the configuration is correct and works as expected by performing these tasks:

Verifying the Network Analytics Configuration

Purpose

Verify the configuration for network analytics.

Action

From operational mode, enter the **show analytics configuration** command to display the traffic and queue monitoring configuration.

`user@host>` **show analytics configuration**

```
Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Enabled, Poll interval: 10 milliseconds
   Depth threshold high: 0 bytes, low: 0 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)           (microseconds)
xe-0/0/1     Enabled      Auto            0         0          900       300
```

Meaning

The output displays information about traffic and queue monitoring on the switch.

Verifying the Network Analytics Status

Purpose

Verify the network analytics operational status of the switch.

Action

From operational mode, enter the **show analytics status** command to display the traffic and queue monitoring status.

```
user@host> show analytics status
```

```
Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Auto, Poll interval: 10 milliseconds
   Depth threshold high: 1228800 bytes, low: 1024 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)           (microseconds)
xe-0/0/1     Enabled       Auto          1228800   1024         900       300
xe-0/0/7     Auto          Auto          1228800   1024         900       300
xe-0/0/8     Auto          Auto          1228800   1024         900       300
```

Verifying Streaming Servers Configuration

Purpose

Verify the configuration for streaming data to remote servers is working.

Action

From operational mode, enter the **show analytics streaming-servers** command to display the streaming servers configuration.

```
user@host> show analytics streaming-servers
```

```
Address        Port     Stream-Format    Stream-Type   State         Sent
10.94.198.11   50001    json             QS            Established   1100
10.94.198.11   50005    csv              TS/QS         In Progress      0
```

Meaning

The output displays information about the remote streaming server.

Verifying Queue Statistics

Purpose

Verify that queue statistics collection is working.

Action

From operational mode, enter the **show analytics queue-statistics** command to display the queue statistics.

```
user@host> show analytics queue-statistics
```

```
Time               Interface   Queue-length (bytes)   Latency (us)
Apr 6 0:17:18.224  xe-0/0/1            1043952            835
Apr 6 0:17:18.234  xe-0/0/1            1053520            842
Apr 6 0:17:18.244  xe-0/0/1            1055184            844
```

Meaning

The output displays queue-statistics information as expected.

Verifying Traffic Statistics

Purpose

Verify that traffic statistics collection is working.

Action

From operational mode, enter the **show analytics traffic-statistics** command to display the traffic statistics.

```
user@host> show analytics traffic-statistics
```

```
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/1
  Traffic Statistics:                Receive            Transmit
  Total octets:                4797548752936        408886273632
  Total packet:                   5658257464          3190613435
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           252901000
  Packet dropped:                          0              252901
  Utilization:                         0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/7
  Traffic Statistics:                Receive            Transmit
  Total octets:                4790866253100           477139024
  Total packet:                   5624473639              477944
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           166582000
  Packet dropped:                          0              166582
  Utilization:                         0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/8
```

```
Traffic Statistics:                Receive           Transmit
Total octets:                4789797668456          764910024
Total packet:                  5623280870             765715
Octets per second:                      0                  0
Packet per second:                      0                  0
Octets dropped:                         0          156099000
Packet dropped:                         0             156099
Utilization:                         0.0%               0.0%
```

Meaning

The output displays traffic-statistics information as expected.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

Example: Configuring Enhanced Network Analytics Features

IN THIS SECTION

- Requirements | 1160
- Overview | 1161
- Configuration | 1161
- Verification | 1168

This example shows how to configure the enhanced network analytics feature, including queue and traffic monitoring.

Requirements

This example uses the following hardware and software components:

- A QFX5100 standalone switch
- A external streaming server to collect data

- Junos OS Release 13.2X51-D15 software
- TCP server software (for remote streaming servers)

Before you configure network analytics, be sure you have:

- Junos OS Release 13.2X51-D15 or later software installed and running on the QFX5100 switch.
- (Optional for streaming servers for the JSON, CSV, and TSV formats) TCP or UDP server software set up for processing records separated by a newline character (\n) on the remote streaming server.
- (Optional for streaming servers for the GPB format) TCP or UDP build streaming server using the **analytics.proto** file.
- All other network devices running.

Overview

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You enable network analytics by first defining a resource profile template, and then applying the profile to the system (for a global configuration) or to individual interfaces.

> **NOTE:** You can configure queue and traffic monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.
>
> Disabling of the queue or traffic monitoring supersedes the configuration (enabling) of this feature. You disable monitoring by applying a resource profile that includes the **no-queue-monitoring** or **no-traffic-monitoring** configuration statement at the **[edit services analytics resource-profiles]** hierarchy level.

Topology

In this example, the QFX5100 switch is connected to an external server used for streaming statistics data.

Configuration

IN THIS SECTION

- Configuring the Polling Interval for Queue and Traffic Monitoring | **1162**
- Configuring a Local Statistics File | **1163**

- Configuring and Applying a Resource Profile for the System | **1163**
- Configuring and Applying a Resource Profile for an Interface | **1164**
- Configuring an Export Profile and Collector for Streaming Data | **1165**

To configure the network analytics features, perform these tasks:

CLI Quick Configuration

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

```
[edit]
set services analytics resource system polling-interval queue-monitoring 1000
set services analytics resource system polling-interval traffic-monitoring 5
set services analytics collector local file an.stats
set services analytics collector local file an files 3
set services analytics collector local file an size 10m
set services analytics resource-profiles sys-rp queue-monitoring
set services analytics resource-profiles sys-rp traffic-monitoring
set services analytics resource-profiles sys-rp depth-threshold high 999999 low 99
set services analytics resource system resource-profile sys-rp
set services analytics resource-profiles if-rp queue-monitoring
set services analytics resource-profiles if-rp traffic-monitoring
set services analytics resource-profiles if-rp latency-threshold high 2300 low 20
set services analytics resource interfaces xe-0/0/16 resource-profile if-rp
set services analytics resource interfaces xe-0/0/18 resource-profile if-rp
set services analytics resource interfaces xe-0/0/19 resource-profile if-rp
set services analytics export-profiles ep stream-format gpb
set services analytics export-profiles ep interface information
set services analytics export-profiles ep interface statistics queue
set services analytics export-profiles ep interface statistics traffic
set services analytics export-profiles ep interface status link
set services analytics export-profiles ep system information
set services analytics export-profiles ep system status queue
set services analytics export-profiles ep system status traffic
set services analytics collector address 10.94.198.11 port 50001 transport tcp export-profile ep
set services analytics collector address 10.94.184.25 port 50013 transport udp export-profile ep
```

Configuring the Polling Interval for Queue and Traffic Monitoring

Step-by-Step Procedure

To configure the polling interval queue and traffic monitoring globally:

1. Configure the queue monitoring polling interval (in milliseconds) for the system:

```
[edit]
set services analytics resource system polling-interval queue-monitoring 1000
```

2. Configure the traffic monitoring polling interval (in seconds) for the system:

```
[edit]
set services analytics resource system polling-interval traffic-monitoring 5
```

Configuring a Local Statistics File

Step-by-Step Procedure

To configure a file for local statistics collection:

1. Configure the filename:

```
[edit]
set services analytics collector local file an.stats
```

2. Configure the number of files:

```
[edit]
set services analytics collector local file an files 3
```

3. Configure the file size:

```
[edit]
set services analytics collector local file an size 10m
```

Configuring and Applying a Resource Profile for the System

Step-by-Step Procedure

To define a resource profile template for queue and traffic monitoring resources:

1. Configure a resource profile and enable queue monitoring:

```
[edit]
set services analytics resource-profiles sys-rp queue-monitoring
```

2. Enable traffic monitoring in the profile:

```
[edit]
set services analytics resource-profiles sys-rp traffic-monitoring
```

3. Configure the depth-threshold (high and low values) for queue monitoring in the profile:

```
[edit]
set services analytics resource-profiles sys-rp depth-threshold high 999999 low 99
```

4. Apply the resource profile template to the system resource type for a global configuration:

```
[edit]
set services analytics resource system resource-profile sys-rp
```

Configuring and Applying a Resource Profile for an Interface

Step-by-Step Procedure

You can configure queue and traffic monitoring for one or more specific interfaces. The interface-specific configuration supersedes the global (system) configuration. To define a resource profile template for queue and traffic monitoring resources for an interface:

1. Configure a resource profile and enable queue monitoring:

```
[edit]
set services analytics resource-profiles if-rp queue-monitoring
```

2. Enable traffic monitoring in the profile:

```
[edit]
set services analytics resource-profiles if-rp traffic-monitoring
```

3. Configure the latency-threshold (high and low values) for queue monitoring in the profile:

```
[edit]
set services analytics resource-profiles if-rp latency-threshold high 2300 low 20
```

4. Apply the resource profile template to the interfaces resource type for specific interfaces:

```
[edit]
set services analytics resource interfaces xe-0/0/16 resource-profile if-rp
set services analytics resource interfaces xe-0/0/18 resource-profile if-rp
set services analytics resource interfaces xe-0/0/19 resource-profile if-rp
```

Configuring an Export Profile and Collector for Streaming Data

Step-by-Step Procedure

To configure a collector (streaming server) for receiving monitoring data:

1. Create an export profile and specify the stream format:

```
[edit]
set services analytics export-profiles ep stream-format gpb
```

2. Configure the export profile to include interface information:

```
[edit]
set services analytics export-profiles ep interface information
```

3. Configure the export profile to include interface queue statistics:

```
[edit]
set services analytics export-profiles ep interface statistics queue
```

4. Configure the export profile to include interface traffic statistics:

```
[edit]
set services analytics export-profiles ep interface statistics traffic
```

5. Configure the export profile to include interface status link information:

```
[edit]
set services analytics export-profiles ep interface status link
```

6. Configure the export profile to include system information:

```
[edit]
```

```
set services analytics export-profiles ep system information
```

7. Configure the export profile to include system queue status:

```
[edit]
set services analytics export-profiles ep system status queue
```

8. Configure the export profile to include system traffic status:

```
[edit]
set services analytics export-profiles ep system status traffic
```

9. Configure the transport protocol for the collector addresses and apply an export profile:

```
[edit]
set services analytics collector address 10.94.198.11 port 50001 transport tcp export-profile ep
set services analytics collector address 10.94.184.25 port 50013 transport udp export-profile ep
```

> **NOTE:** If you configure the **tcp** or **udp** option for the JSON, CSV, and TSV formats, you must also set up the TCP or UDP client software on the remote collector to process records that are separated by the newline character (\n) on the remote server.
>
> If you configure the **tcp** or **udp** option for the GPB format, you must also set up the TCP or UDP build streaming server using the **analytics.proto** file.

Results

Display the results of the configuration:

```
[edit services analytics]
user@switch# run show configuration
services {
    analytics {
        export-profiles {
            ep {
                stream-format gpb;
                interface {
                    information;
```

```
            statistics {
                traffic;
                queue;
            }
            status {
                link;
            }
        }
        system {
            information;
            status {
                traffic;
                queue;
            }
        }
    }
}
resource-profiles {
    sys-rp {
        queue-monitoring;
        traffic-monitoring;
        depth-threshold high 99999 low 99;
    }
    if-rp {
        queue-monitoring;
        traffic-monitoring;
        latency-threshold high 2300 low 20;
    }
}
resource {
    system {
        resource-profile sys-rp;
        polling-interval {
            traffic-monitoring 5;
            queue-monitoring 1000;
        }
    }
    interfaces {
        xe-0/0/16 {
            resource-profile if-rp;
        }
        xe-0/0/18 {
            resource-profile if-rp;
        }
```

```
            xe-0/0/19 {
               resource-profile if-rp;
            }
         }
      }
      collector {
         local {
            file an size 10m files 3;
         }
         address 10.94.184.25 {
            port 50013 {
               transport udp {
                  export-profile ep;
               }
            }
         }
         address 10.94.198.11 {
            port 50001 {
               transport tcp {
                  export-profile ep;
               }
            }
         }
      }
   }
}
```

Verification

IN THIS SECTION

- Verifying the Network Analytics Configuration | **1169**
- Verifying the Network Analytics Status | **1169**
- Verifying the Collector Configuration | **1170**
- Verifying Queue Statistics | **1171**
- Verifying Traffic Statistics | **1171**

Confirm that the configuration is correct and works as expected by performing these tasks:

Verifying the Network Analytics Configuration

Purpose

Verify the configuration for network analytics.

Action

From operational mode, enter the **show analytics configuration** command to display the traffic and queue monitoring configuration.

```
user@host> show analytics configuration
```

```
Traffic monitoring status is enabled
Traffic monitoring polling interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic       Queue        Queue depth             Latency
            Statistics    Statistics      threshold             threshold
                                        High         Low      High      Low
                                           (bytes)            (nanoseconds)
xe-0/0/16   enabled       enabled        n/a          n/a      2300      20
xe-0/0/18   enabled       enabled        n/a          n/a      2300      20
xe-0/0/19   enabled       enabled        n/a          n/a      2300      20
```

Meaning

The output displays the traffic and queue monitoring configuration information on the switch.

Verifying the Network Analytics Status

Purpose

Verify the network analytics operational status of the switch.

Action

From operational mode, enter the **show analytics status global** command to display global traffic and queue monitoring status.

```
user@host> show analytics status global
```

```
Traffic monitoring status is enabled
Traffic monitoring pollng interval : 5 seconds
Queue monitoring status is enabled
```

```
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes
```

From operational mode, enter the **show analytics status** command to display both the interface and global queue monitoring status.

`user@host>` **show analytics status**

```
Traffic monitoring status is enabled
Traffic monitoring pollng interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic    Queue      Queue depth            Latency
            Statistics Statistics    threshold            threshold
                                   High       Low        High      Low
                                      (bytes)            (nanoseconds)
xe-0/0/16   enabled    enabled     n/a        n/a        2300      20
xe-0/0/18   enabled    enabled     n/a        n/a        2300      20
xe-0/0/19   enabled    enabled     n/a        n/a        2300      20
```

Meaning

The output displays the global and interface status of traffic and queue monitoring on the switch.

Verifying the Collector Configuration

Action

Verify the configuration for the collector for streamed data is working.

From operational mode, enter the **show analytics collector** command to display the streaming servers configuration.

`user@host>` **show analytics collector**

```
Address        Port   Transport  Stream format  State          Sent
10.94.184.25   50013  udp        gpb            n/a            484
10.94.198.11   50001  tcp        gpb            In progress    0
```

Meaning

The output displays the collector configuration.

> **NOTE:** The connection state of a port configured with the **udp** transport protocol is always displayed as **n/a**.

Verifying Queue Statistics

Purpose

Verify that queue statistics collection is working.

Action

From operational mode, enter the **show analytics queue-statistics** command to display the queue statistics.

```
user@host> show analytics queue-statistics
```

```
CLI issued at 2014-03-04 15:37:03.116018
Time                      Interface   Queue-depth   Latency
                                      (bytes)       (nanoseconds)
00:00:00.412371 ago       xe-0/0/19   1384656       1107724
00:00:01.412395 ago       xe-0/0/19   1375712       1100569
00:00:02.415366 ago       xe-0/0/19   1385280       1108224
00:00:03.417395 ago       xe-0/0/19   1381744       1105395
00:00:04.411392 ago       xe-0/0/19   1368432       1094745
00:00:05.414387 ago       xe-0/0/19   1374880       1099904
00:00:06.414365 ago       xe-0/0/19   1373632       1098905
00:00:07.416386 ago       xe-0/0/19   1370096       1096076
00:00:08.413384 ago       xe-0/0/19   1377168       1101734
00:00:09.415379 ago       xe-0/0/19   1370720       1096576
00:00:10.418374 ago       xe-0/0/19   1381120       1104896
00:00:11.410376 ago       xe-0/0/19   1383408       1106726
00:00:12.412372 ago       xe-0/0/19   1382576       1106060
00:00:13.417371 ago       xe-0/0/19   1387152       1109721
00:00:14.411368 ago       xe-0/0/19   1375296       1100236
---(more)---
```

Meaning

The output displays queue-statistics information, with the latest record at the top of the report.

Verifying Traffic Statistics

Purpose

Verify that traffic statistics collection is working.

Action

From operational mode, enter the **show analytics traffic-statistics** command to display the traffic statistics.

`user@host>` **show analytics traffic-statistics**

```
CLI issued at 2014-03-04 15:37:52.047136
Time: 00:00:02.252377 ago, Physical interface: xe-0/0/19
  Traffic Statistics:                Receive            Transmit
  Total octets:                  15044882432       1502607382656
  Total packets:                   117538143         11739120146
  Unicast packet:                  117538143         11739120146
  Multicast packets:                       0                   0
  Broadcast packets:                       0                   0
  Octets per second:                86488360          8649309384
  Packets per second:                  84461             8446590
  CRC/Align errors:                        0                   0
  Packets dropped:                         0         11760298455
Time: 00:00:02.252377 ago, Physical interface: xe-0/0/18
  Traffic Statistics:                Receive            Transmit
  Total octets:                1504619929836         15782818944
  Total packets:                 11754843131           123303273
  Unicast packet:                11754843131           123303273
  Multicast packets:                       0                   0
  Broadcast packets:                       0                   0
  Octets per second:              8649134008            86487816
  Packets per second:                8446458               84461
  CRC/Align errors:                        5                   0
  Packets dropped:                         0                   0
Time: 00:00:02.252377 ago, Physical interface: xe-0/0/16
  Traffic Statistics:                Receive            Transmit
  Total octets:                1504801437048           757345408
  Total packets:                 11756261156             5916761
  Unicast packet:                11756261156             5916761
  Multicast packets:                       0                   0
  Broadcast packets:                       0                   0
  Octets per second:              7910619496                   0
  Packets per second:                7725214                   0
  CRC/Align errors:                        3                   0
  Packets dropped:                         0                   0
```

Meaning

The output displays traffic-statistics information.

RELATED DOCUMENTATION

Network Analytics Overview | 1120

10

PART

Port Mirroring and Analyzers

Overview of Port Mirroring | **1175**

Configuring Port Mirroring Analyzers | **1214**

Configuring Port Mirroring Instances | **1308**

Configuring Port Mirroring for Physical Interfaces | **1322**

Configuring Port Mirroring for Logical Interfaces | **1339**

Configuring Port Mirroring for Multiple Destinations | **1401**

Configuring Port Mirroring for Remote Destinations | **1417**

Configuring Port Mirroring Local and Remote Analysis | **1429**

Monitoring Port Mirroring | **1457**

Troubleshooting Port Mirroring | **1459**

CHAPTER 35

Overview of Port Mirroring

IN THIS CHAPTER

- Understanding Port Mirroring and Analyzers | **1175**
- Understanding Port Mirroring | **1183**
- Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches | **1185**
- Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches | **1191**
- Understanding Port Mirroring on SRX Devices | **1199**
- Understanding Layer 2 Port Mirroring | **1200**
- Understanding Layer 2 Port Mirroring Properties | **1201**
- Application of Layer 2 Port Mirroring Types | **1203**
- Restrictions on Layer 2 Port Mirroring | **1205**
- Port Mirroring Constraints and Limitations | **1206**
- Port Mirroring Constraints and Limitations | **1210**

Understanding Port Mirroring and Analyzers

IN THIS SECTION

- [xref target has no title]
- Port Mirroring Overview | **1176**
- Analyzer Overview | **1177**
- Port-Mirroring Terminology | **1177**
- Port Mirroring Instance Types | **1179**
- Port Mirroring and STP | **1179**
- Port-Mirroring Performance Limitation | **1179**
- Local and Remote Port Mirroring Constraints and Limitations | **1179**

Remote Port Mirroring Constraints and Limitations | 1181
Port Mirroring on OCX Series Switches Constraints and Limitations | 1182

Port mirroring and analyzers send network traffic to devices running analyzer applications. A port mirror copies Layer 3 IP traffic to an interface. An analyzer copies bridged (Layer 2) packets to an interface. Mirrored traffic can be sourced from single or multiple interfaces. You can use a device attached to a mirror output interface running an analyzer application to perform tasks such as monitoring compliance, enforcing policies, detecting intrusions, monitoring network performance, correlating events, and other problems on the network.

Port Mirroring Overview

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, port mirroring copies Unicast packets entering or exiting a port or entering a VLAN and sends those copies to a local interface for local monitoring or to a VLAN for remote monitoring. The mirrored traffic is received by applications that help you analyze that traffic.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine, where a key is placed in a file or cflowd. Packets based on that key are sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through the specified interface where it can be captured and analyzed in detail.

You can configure both traffic sampling and port mirroring, setting an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both traffic sampling and port mirroring, only port mirroring is executed, as it takes precedence. In other words, if you configure an interface to traffic sample every packet input to the interface and port mirroring also selects that packet to be copied and sent to the destination port, only the port mirroring process is executed. Traffic sampled packets that are not selected for port mirroring continue to be sampled and forwarded to the cflowd server.

You can use port mirroring to copy:

- All of the packets entering or exiting an interface in any combination. Copies of packets entering some interfaces and packets exiting other interfaces can be sent to the same local interface or VLAN. If you configure port mirroring to copy packets exiting an interface, traffic that *originates* on that switch or Node device (in a QFabric system) is not copied when it egresses. Only *switched* traffic is copied on egress. (See the limitation on egress mirroring below.)
- Any or all packets entering a VLAN. You cannot use port mirroring to copy packets exiting a VLAN.
- A firewall-filtered sample of packets entering a port or VLAN.

NOTE: Firewall filters are not supported on egress ports; you cannot specify policy-based sampling of packets exiting an interface.

Analyzer Overview

You can configure an analyzer statement to define both the input traffic and output traffic in the same analyzer configuration. The traffic to be analyzed can be traffic that enters or exits an interface, or traffic that enters a VLAN. The analyzer configuration enables you to send this traffic to an output interface, instance, or VLAN. You can configure an analyzer at the **[edit forwarding-options analyzer]** hierarchy.

Port-Mirroring Terminology

Table 136 on page 1177 lists the terms used in the documentation about port mirroring and provides definitions.

Table 136: Port Mirroring Terms and Definitions

Term	Definition
Analyzer instance	Port-mirroring configuration that includes a name, source interfaces or source VLAN, and a destination for mirrored packets (either a local interface or a VLAN).
Port mirroring instance **NOTE:** Port mirroring instance is not supported on NFX150 devices.	A port-mirroring configuration that does not specify an input. A firewall filter must be used to send traffic to the port mirror. Use the **port-mirror-instance *instance-name*** action in the firewall filter configuration to send packets to the port mirror.
Output interface (also known as the monitor interface)	The interface to where the copies of packets are sent and to which a device running an analyzer is connected. The following limitations apply to an output interface (the target mirror interface): • Cannot also be a source port. • Cannot be used for switching. • Cannot be an aggregated Ethernet interface (LAG). • Cannot participate in Layer 2 protocols, such as Spanning Tree Protocol (STP). • Existing VLAN associations are lost when port mirroring is applied to the interface. • Packets are dropped if the capacity of the output interface is insufficient to handle the traffic from the mirrored source ports.

Table 136: Port Mirroring Terms and Definitions *(continued)*

Output IP address	IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature: • Mirrored packets are GRE-encapsulated. The analyzer application must be able to de-encapsulate GRE-encapsulated packets or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer application. (You can use a network sniffer to de-encapsulate the packets.) • The output IP address cannot be in the same subnetwork as any of the switch management interfaces. • If you create virtual routing instances and an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
Output VLAN (also known as monitor or analyzer VLAN)	VLAN to where copies of the packets are sent and to where a device running an analyzer is connected. The analyzer VLAN can span multiple switches. The following limitations apply to an output VLAN: • Cannot be a private VLAN or VLAN range. • Cannot be shared by multiple **analyzer** statements. • Cannot be a member of any other VLAN. • Cannot be an aggregated Ethernet interface (LAG). • On some switches, only one interface can be a member of the analyzer VLAN. This limitation does not apply on the QFX10000 switch. When *ingress* traffic is mirrored, multiple QFX10000 interfaces can belong to the output VLAN and traffic is mirrored from all of those interfaces. If *egress* traffic is mirrored on a QFX10000 switch, only one interface can be a member of the analyzer VLAN.
Input interface (also known as mirrored or monitored interface)	An interface that copies traffic to the mirror interface. This traffic can be entering or exiting (ingress or egress) the interface. A mirrored input interface cannot be used as an output interface to the analyzer device.
Monitoring station	A computer running an analyzer application.
Local port mirroring	A port-mirroring configuration where the mirrored packets are copied to an interface on the same switch.
Remote port mirroring	Mirrored packets are sent to an output (analyzer) VLAN that you create to receive mirror traffic or to a remote IP address. (You cannot send mirrored packets to a remote IP address on a QFabric system.)
Policy-based mirroring	Mirroring of packets that match a firewall filter term. The action **analyzer *analyzer-name*** is used in the firewall filter to send specified packets to the analyzer.

Port Mirroring Instance Types

To configure port mirroring, configure an instance of one of the following types:

- Analyzer instance—Specify the input and output for the instance. This instance type is useful for ensuring that all traffic transiting an interface or entering a VLAN is mirrored and sent to the analyzer.
- Port-mirroring instance—You create a firewall filter that identifies the desired traffic and copies it to the mirror port. You do not specify an input for this instance type. This instance type is useful for controlling the types of traffic that are mirrored. You can direct traffic to it in the following ways:
  - Specify the name of the port-mirroring instance in the firewall filter by using the **port-mirror-instance *instance-name*** action when there are multiple port-mirroring instances defined.
  - Send the mirrored packets to the output interface defined in the instance by using the **port-mirror** action when there is only one port-mirroring instance defined.

Port Mirroring and STP

The behavior of STP in a port-mirroring configuration depends on the version of Junos OS you are using:

- Junos OS 13.2X50, Junos OS 13.2X51-D25 or earlier, Junos OS 13.2X52: When STP is enabled, port mirroring might not succeed because STP might block the mirrored packets.
- Junos OS 13.2X51-D30, Junos OS 14.1X53: STP is disabled for mirrored traffic. You must ensure that your topology prevents loops of this traffic.

Port-Mirroring Performance Limitation

Mirroring only the packets required for analysis reduces the possibility of reducing overall performance. If you mirror traffic from multiple ports, the mirrored traffic might exceed the capacity of the output interface. The overflow packets are dropped. We recommend that you limit the amount of mirrored traffic by selecting specific interfaces and avoid using the **all** keyword. You can also limit the amount of mirrored traffic by using a firewall filter to send specific traffic to the port mirroring instance.

Local and Remote Port Mirroring Constraints and Limitations

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.
- Each Node group in a QFabric system is subject to the following constraints:
  - Up to four of the configurations can be used for local port mirroring.
  - Up to three of the configurations can be used for remote port mirroring.

- Regardless of whether you are configuring a standalone switch or a Node group:
  - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
  - There can be no more than two configurations that mirror egress traffic.
  - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- Configure mirroring in an analyzer (with **set forwarding-options analyzer**) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.
- If you mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are not sent to the output port or VLAN.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.
- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.

- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies will have incorrect VLAN IDs.

  This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the same Node device. In this case the mirrored copies will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5xxx (including QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210) and EX4600 (including EX4600 and EX4650) switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.
- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.
- Egress VLAN mirroring is not supported.

Remote Port Mirroring Constraints and Limitations

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, that address cannot be in the same subnetwork as any of the switch management interfaces.
- If you create virtual routing instances and you create an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.
- If the output VLAN has more than one member interface, then traffic is mirrored only to the first member of the VLAN, and other members of the same VLAN do not carry any mirrored traffic.
- If you attempt to configure more than one analyzer session for remote port mirroring to an IP address (GRE encapsulation) and the IP addresses of the analyzers are reachable through the same interface, then only one analyzer session is configured.

- The number of possible output interfaces in remote port mirroring varies among the switches in the QFX5K line:
  - QFX5110, QFX5120, QFX5210—Support a maximum of 4 output interfaces
  - QFX5100 and QFX5200—Support a maximum of 3 output interfaces.
- Whenever any member in a remote port mirroring VLAN is removed from that VLAN, reconfigure the analyzer session for that VLAN.

Port Mirroring on OCX Series Switches Constraints and Limitations

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. There can be no more than two configurations that mirror ingress or egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces by using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

RELATED DOCUMENTATION

Configuring Port Mirroring | 1429
Examples: Configuring Port Mirroring for Local Analysis | 1436
Examples: Configuring Port Mirroring for Local Analysis | 1436
Example: Configuring Port Mirroring for Remote Analysis | 1450
Troubleshooting Port Mirroring | 1459

Understanding Port Mirroring

IN THIS SECTION

Port Mirroring Overview | 1183
Port-Mirroring Terminology | 1183

Port Mirroring Overview

Use port mirroring to send traffic to devices that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring is needed when you want to perform traffic analysis because a switch normally sends packets only to the port to which the destination device is connected. You probably do not want to send the original packets for analysis before they are forwarded because of the delay that this would cause, so the common alternative is to configure port mirroring to send copies of unicast traffic to another interface and run an analyzer application on a device connected to that interface. .

To configure port mirroring, you configure a port-mirroring instance. You do not specify an input for this instance. Instead, you create a firewall filter that specifies the required traffic and directs it to the instance by including the **port-mirror** action in a **then** term of the filter. The firewall filter must be configured as **family inet**.

Keep performance in mind when configuring port mirroring. Configuring the firewall filter to mirror only the necessary packets reduces the possibility of a performance impact.

Port-Mirroring Terminology

Table 136 on page 1177 lists the terms used in the documentation about port mirroring and provides definitions.

Table 137: Port Mirroring Terms and Definitions

Term	Description
Port mirroring instance	A port-mirroring configuration that does not specify an input.. A firewall filter must be used to send traffic to the port mirror. Use the action **port-mirror** action in the firewall filter configuration to send packets to the port mirror.
Output interface (also known as monitor interface)	Access interface to which packet copies are sent and to which a device running an analyzer application is connected. The following limitations apply to an output interface: • Cannot also be a source port. • Cannot be used for switching. • Cannot be an aggregated Ethernet interface (LAG). If the capacity of the output interface is insufficient to handle the traffic from the source ports, overflow packets are dropped.
Output IP address	IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) • An output IP address cannot be in the same subnetwork as any of the switch's management interfaces. • If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).
Monitoring station	Computer running an analyzer application.
Local port mirroring	Port-mirroring configuration in which the mirrored packets are sent to an interface on the same switch.

RELATED DOCUMENTATION

Configuring Port Mirroring

Example: Mirroring Employee Web Traffic with a Firewall Filter | 1351

Troubleshooting Port Mirroring | 1459

Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

IN THIS SECTION

- Port Mirroring Overview | 1185
- Analyzer Configuration | 1186
- Port Mirroring and Analyzer Terminologies | 1186
- Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches | 1188
- Port-Mirroring Limitation | 1191

Mirroring might be needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected.

Junos OS running on EX2300, EX3400, and EX4300 Series switches supports the Enhanced Layer 2 Software (ELS) configurations that facilitate analyzing traffic on these switches at the packet level.

You use port mirroring to copy packets to a local interface for local monitoring or to a VLAN for remote monitoring. You can use analyzers to enforce policies concerning network usage and file sharing, and to identify sources of problems on your network by locating abnormal or heavy bandwidth usage by specific stations or applications.

Port Mirroring Overview

Port mirroring is configured at the **[edit forwarding-options port-mirroring]** hierarchy level. To mirror routed (Layer 3) packets, you can use the port mirroring configuration in which the **family** statement is set to **inet** or **inet6**.

You can use port mirroring to copy these packets:

- **Packets entering or exiting a port**—You can mirror the packets in any combination of packets entering or exiting ports up to 256 ports.

  In other words, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.

- **Packets entering a VLAN**—You can mirror the packets entering a VLAN to either a local analyzer port or to an analyzer VLAN. You can configure up to 256 VLANs, including a VLAN range and PVLANs, as ingress input to an analyzer.

- **Policy-based sample packets**—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a firewall filter to establish a policy to select the packets to be mirrored and send the sample to a port-mirroring instance or to an analyzer VLAN.

You can configure port mirroring on the switch to send copies of Unicast traffic to an output destination such as an interface, a routing-instance, or a VLAN. Then, you can analyze the mirrored traffic by using a protocol analyzer application. The protocol analyzer application can run either on a computer connected to the analyzer output interface or on a remote monitoring station. For the input traffic, you can configure a firewall filter term to specify whether port mirroring must be applied to all packets at the interface to which the firewall filter is applied. You can apply a firewall filter configured with the action **port-mirror** or **port-mirror-instance *name*** to the input or output logical interfaces (including aggregated Ethernet logical interfaces), to traffic forwarded or flooded to a VLAN, or traffic forwarded or flooded to a VPLS routing instance. EX2300, EX3400, and EX4300 switches support port mirroring of VPLS (**family ethernet-switching** or **family vpls**) traffic and VPN traffic with **family ccc** in a Layer 2 environment.

Within a firewall filter term, you can specify the port-mirroring properties under the **then** statement in the following ways:

- Implicitly reference the port-mirroring properties in effect on the port.
- Explicitly reference a particular named instance of port mirroring.

Analyzer Configuration

You can configure an analyzer at the **[edit forwarding-options analyzer]** hierarchy.

Port Mirroring and Analyzer Terminologies

Table 136 on page 1177 lists the terms used in the documentation about port mirroring and provides definitions.

Table 138: Port Mirroring Terms and Definitions

Term	Definition
Analyzer	In a mirroring configuration (analyzer) on an EX2300, EX3400, or EX4300 switch, the analyzer includes: • The name of the analyzer • Source (input) ports or VLAN (optional)

Table 138: Port Mirroring Terms and Definitions *(continued)*

Analyzer output interface (Also known as monitor port)	Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected. **NOTE:** Interfaces used as output for an analyzer must be configured as family ethernet-switching. Analyzer output interfaces have the following limitations: • Cannot also be a source port. • Cannot be used for switching. • Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port mirroring configuration. • If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
Analyzer VLAN (Also known as monitor VLAN)	VLAN to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN are spread across the switches in your network.
Bridge-domain-based analyzer	An analyzer session configured to use bridge domains for input, output or both.
Default analyzer	An analyzer with default mirroring parameters. By default, the mirroring rate is 1 and the maximum packet length is the length of the complete packet.
Port mirroring	A port-mirroring configuration that does not specify an input source; it specifies only an output destination. A firewall filter configuration must be defined for the input source. A firewall filter configuration must be defined to mirror packets that match the match conditions defined in the firewall filter term. The action item port-mirror-instance instance-name in the firewall filter configuration is used to send packets to the analyzer and these packets form the input source.
Global port mirror	A port mirroring configuration that does not have an instance name. The firewall filter action port-mirror will be the action for the firewall filter configuration.
Input interface (Also known as mirrored ports or monitored interfaces)	An interface on the switch that is being mirrored. Traffic that is either entering or exiting the interface is mirrored.
LAG-based analyzer	An analyzer that has a link aggregation group (LAG) specified as the input (ingress) interface in the analyzer configuration.
Local mirroring	An analyzer configuration in which packets are mirrored to a local analyzer port.
Monitoring station	A computer running a protocol analyzer application.

Table 138: Port Mirroring Terms and Definitions *(continued)*

Analyzer based on next-hop group	An analyzer configuration that uses the next-hop group as the output to an analyzer.
Native analyzer session	An analyzer session that has both input and output definitions in its analyzer configuration.
Policy-based mirroring	Mirroring of packets that match the match items in the defined firewall filter term. The action item port-mirror-instance instance-name is used in the firewall filter to send the packets to the monitor port.
Port-based analyzer	An analyzer session whose configuration defines interfaces for both input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.
Remote port mirroring	Functions the same as local port mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic.
VLAN-based analyzer	An analyzer session whose configuration uses VLANs for both input and output or for either input or output.

Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

When you configure port mirroring we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from mirroring. Additionally, we recommend that you disable mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is, select specific interfaces as input to the analyzer) in preference to using the **all** keyword option that enables mirroring on all interfaces and can impact overall performance. Mirroring only the necessary packets reduces any potential performance impact.

With local mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. Thus, while configuring an analyzer, you must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 139 on page 1189 summarizes additional configuration guidelines for mirroring on EX2300, EX3400, and EX4300 switches.

Table 139: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

Guideline	Value or Support Information	Comment
Number of VLANs that you can use as ingress input to an analyzer.	256	
Number of port-mirroring sessions and analyzers that you can enable concurrently.	4	You can configure a total of four sessions and you can enable only one of the following at any point in time: • A maximum of four port-mirroring sessions (including the global port-mirroring session). See Table 136 on page 1177 for a description of global port mirror. • A maximum of four analyzer sessions. • A combination of port-mirroring and analyzer sessions, and the total of this combination must be four. You can configure more than the specified number of port-mirroring instances or analyzers on the switch, but you can enable only the specified number for a session.
Types of ports on which you cannot mirror traffic.	• Virtual Chassis ports (VCPs) • Management Ethernet ports (me0 or vme0) • Integrated routing and bridging (IRB) interfaces; also known as routed VLAN interfaces (RVIs). • VLAN-tagged Layer 3 interfaces	
Protocol families that you can include in a port-mirroring configuration for remote traffic.	**any**	

Table 139: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches *(continued)*

Guideline	Value or Support Information	Comment
Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations.	Ingress and egress	
Mirrored packets exiting an interface that reflect rewritten class-of-service (CoS) DSCP or 802.1p bits.	Applicable	
Packets with physical layer errors.	Applicable	Packets with these errors are filtered out and thus are not sent to the analyzer.
Port mirroring does not support line-rate traffic.	Applicable	Port mirroring for line-rate traffic is done on a best-effort basis.
Mirroring of packets egressing a VLAN.	Not supported	
Port-mirroring or analyzer output on a LAG interface.	Supported	
Maximum number of child members on a port-mirroring or analyzer output LAG interface.	8	
Maximum number of interfaces in a remote port-mirroring or analyzer VLAN.	1	
Egress mirroring of host-generated control packets.	Not Supported	
Configuring Layer 3 logical interfaces in the **input** stanza of an analyzer.	Not supported	This functionality can be achieved by configuring port mirroring.
The analyzer input and output stanzas containing members of the same VLAN or the VLAN itself must be avoided.	Applicable	

Port-Mirroring Limitation

- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress switched port. Because the processor on EX2300 and EX3400 switches implements egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry VLAN tags that differ from the tags in the original traffic.

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**

Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches

IN THIS SECTION

- Port Mirroring Overview | **1192**
- Port Mirroring Terminology | **1193**
- Configuration Guidelines for Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches | **1195**

Juniper Networks Junos operating system (Junos OS) running on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 or EX8200 Series switches does not support Enhanced Layer 2 Software (ELS) configurations. As such, Junos OS does not include the **port-mirroring** statement found at the **edit forwarding-options** level of the hierarchy of other Junos OS packages, or the **port-mirror** action in firewall filter terms. See "Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches" on page 1185 for port mirroring information on these switches.

You can use port mirroring to facilitate analyzing traffic on your Juniper Networks EX Series Ethernet Switch on a packet level. You might use port mirroring as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing and for identifying sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

You can use port mirroring to copy these packets to a local interface or to a VLAN:

- Packets entering or exiting a port
- You can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- Packets entering a VLAN on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switches
- Packets exiting a VLAN on EX8200 switches

This topic describes:

Port Mirroring Overview

Port mirroring is used for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected.

You configure port mirroring on the switch to send copies of Unicast traffic to either a local analyzer port or an analyzer VLAN. Then you can analyze the mirrored traffic by using a protocol analyzer. The protocol analyzer can run either on a computer connected to the analyzer output interface or on a remote monitoring station.

You can use port mirroring to mirror any of the following:

- **Packets entering or exiting a port**—You can mirror the packets in any combination of packets entering or exiting ports up to 256 ports.

  In other words, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.

- **Packets entering a VLAN on an EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switch**—You can mirror the packets entering a VLAN on an analyzer VLAN. On EX3200, EX4200, EX4500, and EX4550 switches, you can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANs, as ingress input to an analyzer.

- **Packets exiting a VLAN on an EX8200 switch**—You can mirror the packets exiting a VLAN on an EX8200 switch to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANs, as egress input to an analyzer.
- **Statistical samples**—You can mirror a statistical sample of packets that are:
  - Entering or exiting a port
  - Entering a VLAN on an EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switch
  - Exiting a VLAN on an EX8200 switch

  You specify the sample number of packets by setting the ratio. You can send the sample to either a local analyzer port or to an analyzer VLAN.
- **Policy-based sample**—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a firewall filter to establish a policy to select the packets to be mirrored. You can send the sample to a local analyzer port or to an analyzer VLAN.

Port Mirroring Terminology

Table 136 on page 1177 lists the terms used in the documentation about port mirroring and provides definitions.

Table 140: Port Mirroring Terms and Definitions

Term	Definition
Analyzer	A port mirroring configuration on an EX Series switch. The analyzer includes: • The name of the analyzer • Source (input) ports or VLAN (optional) • A destination for mirrored packets (either a monitor port or a monitor VLAN) • Ratio field for specifying statistical sampling of packets (optional) • Loss-priority setting

Table 140: Port Mirroring Terms and Definitions *(continued)*

Analyzer output interface (Also known as monitor port)	Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected. **NOTE:** Interfaces used as output for an analyzer must be configured as family ethernet-switching. Analyzer output interfaces have the following limitations: • Cannot also be a source port. • Cannot be used for switching. • Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port mirroring configuration. • Do not retain any VLAN associations they held before they were configured as analyzer output interfaces. If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
Analyzer VLAN (Also known as monitor VLAN)	VLAN to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN are spread across the switches in your network.
Firewall-based analyzer	An analyzer whose configuration does not specify an input source; it specifies only an output destination. A firewall-based analyzer must be used with a firewall filter to achieve the functionality of an analyzer.
Global analyzer (on EX4500 and EX4550 switches only)	An analyzer that is based on a firewall filter, VLAN, or link aggregation group (LAG) or an analyzer in which interfaces are on different port groups on the switch. A port group is a logical group of ports on the switch.
Input interface (Also known as mirrored ports or monitored interfaces)	An interface on the switch that is being mirrored, on traffic that is either entering or exiting the interface. An input interface cannot also be an output interface for an analyzer.
LAG-based analyzer	An analyzer that has a LAG specified as the input (ingress) interface in the analyzer configuration.
Local port mirroring	An analyzer configuration in which packets are mirrored to a local analyzer port.
Mirror ratio	See statistical sampling.
Monitoring station	A computer running a protocol analyzer application.

Table 140: Port Mirroring Terms and Definitions *(continued)*

Native analyzer session	An analyzer session that has both input and output definitions in its analyzer configuration.
Policy-based mirroring	Mirroring of packets that match the match items in the defined firewall filter term. The action item analyzer analyzer-name is used in the firewall filter to send the packets to the analyzer.
Port-based analyzer	An analyzer session whose configuration defines interfaces for both input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.
Remote port mirroring	Functions the same as local port mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic. If you are using an intermediate (transit) switch, you can avoid flooding of the mirrored traffic to member interfaces of the VLAN by setting the ingress option to specify an interface of the VLAN for ingress-only traffic and the egress option to specify an interface of the VLAN for egress-only traffic in the [edit vlans] hierarchy level.
Statistical sampling	You can configure the system to mirror a sampling of the packets by setting a ratio of 1:x, where x is a value from 1 through 2047. For example, when x is set to 1, all packets are copied to the analyzer. When x is set to 200, 1 of every 200 packets is copied.
VLAN-based analyzer	An analyzer session whose configuration uses VLANs for both input and output or for either input or output.

Configuration Guidelines for Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches

When you configure port mirroring, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from the port mirroring feature. Additionally, we recommend that you disable port mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is, select specific interfaces as input to the analyzer) as opposed to using the **all** keyword that enables port mirroring on all interfaces and can impact overall performance. You can also limit the amount of mirrored traffic by using statistical sampling, setting a ratio to select a statistical sample, or using a firewall filter. Mirroring only the necessary packets reduces any potential performance impact.

With local port mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. Thus, while configuring an analyzer, you must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 139 on page 1189 summarizes further configuration guidelines for port mirroring on the switches.

> **NOTE:** "All other switches" or "All switches" in the description apply to all switch platforms that support port mirroring. For details on platform support, see Feature Explorer.

Table 141: Configuration Guidelines for Port Mirroring

Guideline	Description	Comment
Number of VLANs that you can use as ingress input to an analyzer	• 1—EX2200 switches • 256—EX3200, EX4200, EX4500, EX4550, and EX6200 switches • Does not apply—EX8200 switches	
Number of analyzers that you can enable concurrently (applies to both standalone switches and to Virtual Chassis)	• 1—EX2200, EX3200, EX4200, EX3300, and EX6200 switches • 7 port-based or 1 global—EX4500 and EX4550 switches • 7 total, with one based on a VLAN, firewall filter, or LAG and with the remaining 6 based on firewall filters—EX8200 switches **NOTE:** An analyzer configured using a firewall filter does not support mirroring of packets that are egressing ports.	• You can *configure* more than the specified number of analyzers on the switch, but you can *enable* only the specified number for a session. Use **disable ethernet-switching-options analyzer name** to disable an analyzer. • See Table 136 on page 1177 for a description of global analyzers. • See the next row entry in this table for the exception to the number of firewall-filter–based analyzers allowed on EX4500 and EX4550 switches. • On an EX4550 Virtual Chassis, you can configure only one analyzer if ports in the input and output definitions are on different switches in a Virtual Chassis. To configure multiple analyzers, an entire analyzer session must be configured on the same switch of a Virtual Chassis.

Table 141: Configuration Guidelines for Port Mirroring *(continued)*

Guideline	Description	Comment
Number of firewall-filter–based analyzers that you can configure on EX4500 and EX4550 switches	• 1—EX4500 and EX4550 switches	If you configure multiple analyzers, you cannot attach any of them to a firewall filter.
Types of ports on which you cannot mirror traffic	• Virtual Chassis ports (VCPs) • Management Ethernet ports (me0 or vme0) • Routed VLAN interfaces (RVIs) • VLAN-tagged Layer 3 interfaces	
If port mirroring is configured to mirror packets exiting 10-Gigabit Ethernet ports on EX8200 switches, packets are dropped in both network and mirrored traffic when the mirrored packets exceed 60 percent of the 10-Gigabit Ethernet port traffic.	• EX8200 switches	
Traffic directions for which you can specify a ratio	• Ingress only—EX8200 switches • Ingress and egress—All other switches	
Protocol families that you can include in a firewall-filter-based remote analyzer	• Any except **inet** and **inet6**—EX8200 switches • Any—All other switches	You can use **inet** and **inet6** on EX8200 switches in a local analyzer.
Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations	• Ingress only—All switches	
Mirrored packets on tagged interfaces might contain an incorrect VLAN ID or Ethertype.	• Both VLAN ID and Ethertype—EX2200 switches • VLAN ID only—EX3200 and EX4200 switches • Ethertype only—EX4500 and EX4550 switches • Does not apply—EX8200 switches	

Table 141: Configuration Guidelines for Port Mirroring *(continued)*

Guideline	Description	Comment
Mirrored packets exiting an interface do not reflect rewritten class-of-service (CoS) DSCP or 802.1p bits.	• All switches	
The analyzer appends an incorrect 802.1Q (**dot1q**) header to the mirrored packets on the routed traffic or does not mirror any packets on the routed traffic when an egress VLAN that belongs to a routed VLAN interface (RVI) is configured as the input for that analyzer.	• EX8200 switches • Does not apply—All other switches	As a workaround, configure an analyzer that uses each port (member interface) of the VLAN as egress input.
Packets with physical layer errors are not sent to the local or remote analyzer.	• All switches	Packets with these errors are filtered out and thus are not sent to the analyzer.
Port mirroring configuration on a Layer 3 interface with the output configured to a VLAN is not available on EX8200 switches.	• EX8200 switches • Does not apply—All other switches	
Port mirroring does not support line-rate traffic.	• All switches	Port mirroring for line-rate traffic is done on a best-effort basis.
In an EX8200 Virtual Chassis, to mirror traffic across the Virtual Chassis, the output port must be a LAG.	• EX8200 Virtual Chassis • Does not apply—All other switches	In an EX8200 Virtual Chassis: • You can configure LAG as a monitor port only for native analyzers. • You cannot configure LAG as a monitor port for analyzers based on firewall filters. • If an analyzer configuration contains LAG as a monitor port, then you cannot configure VLAN in the input definition of an analyzer.

Table 141: Configuration Guidelines for Port Mirroring *(continued)*

Guideline	Description	Comment
In standalone EX8200 switches, you can configure LAG in the output definition.	• EX8200 standalone switches • Does not apply—All other switches	In EX8200 standalone switches: • You can configure a LAG as a monitor port on both native and firewall-based analyzers. • If a configuration contains LAG as a monitor port, then you cannot configure VLAN in the input definition of an analyzer.

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches

Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches

Understanding Port Mirroring on SRX Devices

Port mirroring copies packets entering or exiting a port and sends the copies to a local interface for monitoring. Port mirroring is used to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. </para><para>Port mirroring is used to send a copy of all the packets or only the sampled packets seen on a port to a network monitoring connection. You can mirror the packets either on the incoming port (ingress port mirroring) or the outgoing port (egress port mirroring).

Port mirroring is supported only on the SRX devices with the following I/O cards:

- SRX1K-SYSIO-GE
- SRX1K-SYSIO-XGE
- SRX3K-SFB-12GE
- SRX3K-2XGE-XFP
- SRX5K-FPC-IOC Flex I/O

On SRX devices, all packets passing through the **mirrored** port are copied and sent to the specified **mirror-to** port. These ports must be on the same Broadcom chipset in the I/O cards.

On SRX devices, port mirroring works on physical interfaces only.

Understanding Layer 2 Port Mirroring

On routing platforms and switches that contain an Internet Processor II ASIC, you can send a copy of any incoming packet from the routing platform or switch to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

In Junos OS Release 9.3 and later, Juniper Networks MX Series 5G Universal Routing Platforms in a Layer 2 environment support port mirroring for Layer 2 bridging traffic and virtual private LAN service (VPLS) traffic.

In Junos OS Release 9.4 and later, MX Series routers in a Layer 2 environment support port mirroring for Layer 2 VPN traffic over a circuit cross-connect (CCC) that transparently connects logical interfaces of the same type.

In Junos OS Release 12.3R2, Juniper Networks EX Series switches support port mirroring for Layer 2 bridging traffic.

Layer port mirroring enables you to specify the manner in which incoming and outgoing packets at specified ports are monitored and the manner in which copies of selected packets are forwarded to another destination, where the packets can be analyzed.

MX Series routers and EX Series switches support Layer 2 port mirroring by performing flow monitoring functions by using a class-of-service (CoS) architecture that is in concept similar to, but in particular different from, other routing platforms and switches.

Like the M120 Multiservice Edge Router and M320 Multiservice Edge Router, MX Series routers and EX Series switches support the mirroring of IPv4, IPv6, and VPLS packets simultaneously.

In a Layer 3 environment, MX Series routers and EX Series switches support the mirroring of IPv4 (**family inet**) and IPv6 (**family inet6**) traffic. For information about Layer 3 port mirroring, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring Properties | **1201**

Restrictions on Layer 2 Port Mirroring

Application of Layer 2 Port Mirroring Types

Application of Layer 2 Port Mirroring Types

Understanding Layer 2 Port Mirroring Properties

IN THIS SECTION

- Packet-Selection | 1201
- Packet Address Family | 1201
- Mirror Destination Properties | 1202
- Mirror-Once Option | 1202

Port mirroring specifies the following types of properties:

Packet-Selection

The packet-selection properties of Layer 2 port-mirroring specify how the sampled packets are to be selected for mirroring:

- The number of packets in each sample.
- The number of packets to mirror from each sample.
- The length to which mirrored packets are to be truncated.

Packet Address Family

The packet address family type specifies the type of traffic to be mirrored. In a Layer 2 environment, MX Series routers and EX Series switches support port mirroring for the following packet address families:

- Family type **ethernet-switching**—For mirroring VPLS traffic when the physical interface is configured with encapsulation type **ethernet-bridge**.
- Family type **ccc**—For mirroring Layer 2 VPN traffic.
- Family type **vpls**—For mirroring VPLS traffic.

> **NOTE:** In typical applications, you send mirrored packets directly to an analyzer, not to another router or switch. If you must send mirrored packets over a network, you should use tunnels. For Layer 2 VPN implementations, you can use the Layer 2 VPN routing instance type **l2vpn** to tunnel the packets to a remote destination.

For information about configuring a routing instance for Layer 2 VPN, see the *Junos OS VPNs Library for Routing Devices*. For a detailed Layer 2 VPN example configuration, see *Junos OS*. For information about tunnel interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

Mirror Destination Properties

For a given packet address family, the mirror destination properties of a Layer 2 port-mirroring instance specify how the selected packets are to be sent on a particular physical interface:

- The physical interface on which to send the selected packets.
- Whether filter checking is to be disabled for the mirror destination interface. By default, filter checking is enabled on all interfaces.

> **NOTE:** If you apply a filter to an interface that is also a Layer 2 port-mirroring destination, a commit failure occurs unless you have disabled filter checking for that mirror destination interface.

Mirror-Once Option

If port mirroring is enabled at both ingress and egress interfaces, you can prevent the MX Series router and an EX Series switch from sending duplicate packets to the same destination (which would complicate the analysis of the mirrored traffic).

> **NOTE:** The mirror-once port-mirroring option is a global setting. The option is independent of the packet selection properties and the packet family type-specific mirror destination properties.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Restrictions on Layer 2 Port Mirroring

Application of Layer 2 Port Mirroring Types

Application of Layer 2 Port Mirroring Types

You can apply different sets of Layer 2 port-mirroring properties to the VPLS packets at different ingress or egress points of an MX Series or of an EX Series route.

Table 142 on page 1203 describes the three types of Layer 2 port mirroring that you can configure on an MX Series routers and EX Series switches, the: global instance, named instances, and firewall filters.

Table 142: Application of Layer 2 Port Mirroring Types

Type of Layer2PortMirroring Definition	Point of Application	Scope of Mirroring	Description	Configuration Details
Global Instance of Layer2PortMirroring	All ports in the MX Series router (or switch) chassis.	VPLS packets received on all ports in the MX Series router (or switch) chassis.	If configured, the global port-mirroring properties implicitly apply to all the VPLS packets received on all ports in the router (or switch) chassis.	See *Configuring the Global Instance of Layer 2 Port Mirroring*
Named Instance of Layer2PortMirroring	Ports grouped at the FPC level See "Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level" on page 1324.	VPLS packets received on ports associated with a specific DPC or FPC and its Packet Forwarding Engines.	Overrides any port-mirroring properties configured by the global port-mirroring instance.	See *Defining a Named Instance of Layer 2 Port Mirroring*. The number of port-mirroring destinations supported for an MX Series router and for an EX Series switch are limited to the number of Packet Forwarding Engines contained on the DPCs or FPCs installed in the router or switch chassis.
	Ports grouped at the PIC level See "Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level" on page 1326.	VPLS packets received on ports associated with a specific Packet Forwarding Engine.	Overrides any port-mirroring properties configured at the FPC level or in the global port-mirroring instance.	

Table 142: Application of Layer 2 Port Mirroring Types *(continued)*

Type of Layer2PortMirroring Definition	Point of Application	Scope of Mirroring	Description	Configuration Details
Layer2Port-Mirroring Firewall Filter	Logical interface (including an aggregated Ethernet interface) See "Applying Layer 2 Port Mirroring to a Logical Interface" on page 1367.	VPLS packets received or sent on a logical interface.	In the firewall filter configuration, include *action* and *action-modifier* terms to apply to the packets selected for mirroring: 1. The **accept**action is recommended. 2. Specify port mirroring by Including one of the following modifiers: • The **port-mirror** modifier implicitly references the port-mirroring properties currently bound to the underlying physical interfaces. • The **port-mirror-instance *pm-instance-name*** modifier explicitly references a named instance of port mirroring. 3. (Optional) For tunnel interface input packets only, to mirror the packets to additional destinations, include the **next-hop-group *next-hop-group-name*** modifier. This modifier references a next-hop-group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer).	See "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343. **NOTE:** Layer 2 port-mirroring firewall filters are not supported for logical systems. For mirroring tunnel interface input packets to multiple destinations, also see "Defining a Next-Hop Group for Layer 2 Port Mirroring" on page 1402.
	VLAN forwarding table or flood table See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain" on page 1370.	Layer 2 traffic forwarded or flooded to a VLAN		
	VPLS routing instance forwarding table or flood table See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance" on page 1373.	Layer 2 traffic forwarded or flooded to a VPLS routing instance		

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Restrictions on Layer 2 Port Mirroring

Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface | 1322

Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces | 1356

Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces | 1358

Restrictions on Layer 2 Port Mirroring

The following restrictions apply to Layer 2 port mirroring:

- Only Layer 2 transit data (packets that contain chunks of data transiting the routing platform or switch as they are forwarded from a source to a destination) can be mirrored. Layer 2 local data (packets that contain chunks of data that are destined for or sent by the Routing Engine, such as Layer 2 control packets) are not mirrored.
- If you apply a port-mirroring filter to the output of a logical interface, only Unicast packets are mirrored. To mirror Broadcast packets, Multicast packets, Unicast packets with an unknown destination media access control (MAC) address, or packets with a MAC entry in the destination MAC (DMAC) routing table, apply a filter to the input to the flood table of a VLAN or virtual private LAN service (VPLS) routing instance.
- The mirror destination device should be on a dedicated VLAN and should not participate in any bridging activity; the mirror destination device should not have a bridge to the ultimate traffic destination, and the mirror destination device should not send the mirrored packets back to the source address.
- For either the global port-mirroring instance or a named port-mirroring instance, you can configure only one mirror output interface per port-mirroring instance and packet address family. If you include more than one **interface** statement under the **family (ethernet-switching | ccc | vpls) output** statement, the previous **interface** statement is overridden.
- Layer 2 port-mirroring firewall filtering is not supported for logical systems.

  In a Layer 2 port-mirroring firewall filter definition, the ***action-modifier*** filter (**port-mirror** or **port-mirror-instance *pm-instance-name***) relies on port-mirroring properties defined in the global instance or named instances of Layer 2 port mirroring, which are configured under the **[edit forwarding-options port-mirroring]** hierarchy. Therefore, the ***term*** filter cannot support Layer 2 port mirroring for logical systems.
- For a Layer 2 port mirroring firewall filter in which you implicitly reference Layer 2 port mirroring properties by including the **port-mirror** statement, if multiple named instances of Layer 2 port mirroring

are bound to the underlying physical interface, then only the first binding in the stanza (or the only binding) is used at the logical interface. This is done for backward compatibility.

- Layer 2 port-mirroring firewall filters do not support the use of next-hop subgroups for load-balancing mirrored traffic.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Application of Layer 2 Port Mirroring Types

Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface | 1322

Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces | 1356

Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces | 1358

Port Mirroring Constraints and Limitations

IN THIS SECTION

- Local and Remote Port Mirroring | 1206
- Remote Port Mirroring Only | 1208
- Port Mirroring on OCX Series Switches | 1209

Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.
- Each Node group in a QFabric system is subject to the following constraints:
  - Up to four of the configurations can be used for local port mirroring.
  - Up to three of the configurations can be used for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group:

  - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
  - There can be no more than two configurations that mirror egress traffic.
  - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- Configure mirroring in an analyzer (with **set forwarding-options analyzer**) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.
- If you mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are not sent to the output port or VLAN.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.
- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.

- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies will have incorrect VLAN IDs.

  This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the same Node device. In this case the mirrored copies will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5xxx (including QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210) and EX4600 (including EX4600 and EX4650) switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.
- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.
- Egress VLAN mirroring is not supported.

Remote Port Mirroring Only

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, that address cannot be in the same subnetwork as any of the switch management interfaces.
- If you create virtual routing instances and you create an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.
- If the output VLAN has more than one member interface, then traffic is mirrored only to the first member of the VLAN, and other members of the same VLAN do not carry any mirrored traffic.
- If you attempt to configure more than one analyzer session for remote port mirroring to an IP address (GRE encapsulation) and the IP addresses of the analyzers are reachable through the same interface, then only one analyzer session is configured.
- The number of possible output interfaces in remote port mirroring varies among the switches in the QFX5K line:

  - QFX5110, QFX5120, QFX5210—Support a maximum of 4 output interfaces
  - QFX5100 and QFX5200—Support a maximum of 3 output interfaces.
- Whenever any member in a remote port mirroring VLAN is removed from that VLAN, reconfigure the analyzer session for that VLAN.

Port Mirroring on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. There can be no more than two configurations that mirror ingress or egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces by using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

RELATED DOCUMENTATION

Understanding Port Mirroring | **1183**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1351**

Port Mirroring Constraints and Limitations

IN THIS SECTION

- Local and Remote Port Mirroring | **1210**
- Remote Port Mirroring Only | **1212**
- Port Mirroring on OCX Series Switches | **1213**

Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.
- Each Node group in a QFabric system is subject to the following constraints:
  - Up to four of the configurations can be used for local port mirroring.
  - Up to three of the configurations can be used for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group:
  - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
  - There can be no more than two configurations that mirror egress traffic.
  - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- Configure mirroring in an analyzer (with **set forwarding-options analyzer**) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured

on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.

- If you mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are not sent to the output port or VLAN.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.
- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies will have incorrect VLAN IDs.

  This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the same Node device. In this case the mirrored copies will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5xxx (including QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210) and EX4600 (including EX4600 and EX4650) switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.

- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.
- Egress VLAN mirroring is not supported.

Remote Port Mirroring Only

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, that address cannot be in the same subnetwork as any of the switch management interfaces.
- If you create virtual routing instances and you create an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.
- If the output VLAN has more than one member interface, then traffic is mirrored only to the first member of the VLAN, and other members of the same VLAN do not carry any mirrored traffic.
- If you attempt to configure more than one analyzer session for remote port mirroring to an IP address (GRE encapsulation) and the IP addresses of the analyzers are reachable through the same interface, then only one analyzer session is configured.
- The number of possible output interfaces in remote port mirroring varies among the switches in the QFX5K line:
  - QFX5110, QFX5120, QFX5210—Support a maximum of 4 output interfaces
  - QFX5100 and QFX5200—Support a maximum of 3 output interfaces.
- Whenever any member in a remote port mirroring VLAN is removed from that VLAN, reconfigure the analyzer session for that VLAN.

Port Mirroring on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. There can be no more than two configurations that mirror ingress or egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces by using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

RELATED DOCUMENTATION

Understanding Port Mirroring | **1183**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1351**

Configuring Port Mirroring

CHAPTER 36

Configuring Port Mirroring Analyzers

IN THIS CHAPTER

- Understanding Port Mirroring Analyzers | **1214**
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**
- Configuring Port Mirroring to Analyze Traffic (CLI Procedure) | **1234**
- Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches | **1238**
- Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**
- Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | **1268**
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches | **1277**
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches | **1299**

Understanding Port Mirroring Analyzers

IN THIS SECTION

- Analyzer Overview | **1215**
- Statistical Analyzer Overview | **1216**
- Default Analyzer Overview | **1216**
- Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers | **1216**
- Port Mirroring Analyzer Terminology | **1216**
- Configuration Guidelines for Port Mirroring Analyzers | **1218**

Port mirroring can be used for traffic analysis on routers and switches that, unlike hubs, do not broadcast packets to every port on the destination device. Port mirroring sends copies of all packets or policy-based sample packets to local or remote analyzers where you can monitor and analyze the data.

In the context of port mirroring analyzers, we use the term *switching device*. The term indicates that the device (including routers) is performing a switching function.

You can use analyzers on a packet level to help you:

- Monitor network traffic
- Enforce network usage policies
- Enforce file sharing policies
- Identify the causes of problems
- Identify stations or applications with heavy or abnormal bandwidth usage

You can configure port mirroring to mirror:

- Bridged packets (Layer 2 packets)
- Routed packets (Layer 3 packets)

Mirrored packets can be copied to either a local interface for local monitoring or a VLAN or bridge domain for remote monitoring.

The following packets can be copied:

- **Packets entering or exiting a port**—You can mirror packets entering or exiting ports, in any combination, for up to 256 ports. For example, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- **Packets entering or exiting a VLAN or bridge domain**—You can mirror the packets entering or exiting a VLAN or bridge domain to either a local analyzer port or to an analyzer VLAN or bridge domain. You can configure multiple VLANs (up to 256 VLANs) or bridge domains as ingress inputs to an analyzer, including a VLAN range and private VLANs (PVLANs).
- **Policy-based sample packets**—You can mirror a policy-based sample of packets that are entering a port, VLAN, or bridge domain. You configure a firewall filter with a policy to select the packets to be mirrored. You can send the sample to a port-mirroring instance or to an analyzer VLAN or bridge domain.

This topic describes:

Analyzer Overview

You can configure an analyzer to define both the input traffic and the output traffic in the same analyzer configuration. The input traffic to be analyzed can be either traffic that enters or traffic that exits an interface or VLAN. The analyzer configuration enables you to send this traffic to an output interface,

instance, next-hop group, VLAN, or bridge domain. You can configure an analyzer at the **[edit forwarding-options analyzer]** hierarchy level.

Statistical Analyzer Overview

You can define a set of mirroring properties, such as mirroring rate and maximum packet length for traffic, that you can explicitly bind to physical ports on the router or switch. This set of mirroring properties constitutes a statistical analyzer (also called a non-default analyzer). At this level, you can bind a named instance to the physical ports associated with a specific FPC.

Default Analyzer Overview

You can configure an analyzer without configuring any mirroring properties (such as mirroring rate or maximum packet length). By default, the mirroring rate is set to 1 and the maximum packet length is set to the complete length of the packet. These properties are applied at the global level and need not be bound to a specific FPC.

Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers

You can apply up to two statistical analyzers to the same port groups on the switching device. By applying two different statistical analyzer instances to the same FPC or Packet Forwarding Engine, you can bind two distinct Layer 2 mirroring specifications to a single port group. Mirroring properties that are bound to an FPC override any analyzer (default analyzer) properties bound at the global level on the switching device. Default analyzer properties are overridden by binding a second analyzer instance on the same port group.

Port Mirroring Analyzer Terminology

Table 143 on page 1216 lists some port mirroring analyzer terms and their descriptions.

Table 143: Analyzer Terminology

Term	Description
Analyzer	In a mirroring configuration, the analyzer includes: • The name of the analyzer • Source (input) ports, VLANs, or bridge domains • The destination for mirrored packets (either a local port, VLAN, or bridge domain)
Analyzer output interface (Also known as a monitor port)	Interface where mirrored traffic is sent and a protocol analyzer is connected. Interfaces used as output to an analyzer must be configured under the **forwarding-options** hierarchy level.

Table 143: Analyzer Terminology *(continued)*

Term	Description
	Analyzer output interfaces have the following limitations: • They cannot also be a source port. • They do not participate in Layer 2 protocols, such as the Spanning Tree Protocol (STP). • If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
Analyzer VLAN or bridge domain (Also known as a monitor VLAN or bridge domain)	VLAN or bridge domain to where mirrored traffic is sent to be used by a protocol analyzer. The member interfaces in the monitor VLAN or bridge domain are spread across the switching devices in your network.
Bridge-domain-based analyzer	An analyzer session configured to use bridge domains for input, output or both.
Default analyzer	An analyzer with default mirroring parameters. By default, the mirroring rate is 1 and the maximum packet length is the length of the complete packet.
Input interface (Also known as mirrored ports or monitored interfaces)	An interface on the switching device where the traffic entering or exiting this interface is mirrored.
LAG-based analyzer	An analyzer that has a link aggregation group (LAG) specified as the input (ingress) interface in the analyzer configuration.
Local mirroring	An analyzer configuration in which packets are mirrored to a local analyzer port.
Monitoring station	A computer running a protocol analyzer.
Analyzer based on next-hop group	An analyzer configuration that uses the next-hop group as the output to an analyzer.
Port-based analyzer	An analyzer configuration that defines interfaces for input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called a network analyzer, packet sniffer or probe.
Remote mirroring	Functions the same way as local mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN or bridge domain that you create specifically for the purpose of receiving mirrored traffic. Mirrored packets have an additional outer tag of the analyzer VLAN or bridge domain.

Table 143: Analyzer Terminology *(continued)*

Term	Description
Statistical analyzer (Also known as a non-default analyzer)	A set of mirroring properties that you can explicitly bind to the physical ports on the switch. This set of analyzer properties is known as a statistical analyzer.
VLAN-based analyzer	An analyzer configuration that uses VLANs to deliver the mirrored traffic to the analyzer.

Configuration Guidelines for Port Mirroring Analyzers

When you configure port mirroring analyzers. we recommend that you follow these guidelines to ensure optimum benefit. We recommend that you disable mirroring when you are not using it, and that you select specific interfaces as input to the analyzer rather than using the **all** keyword option, which enables mirroring on all interfaces. Mirroring only necessary packets reduces any potential performance impact.

You can also limit the amount of mirrored traffic by:

- Using statistical sampling
- Using a firewall filter
- Setting a ratio to select a statistical sample

With local mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. You must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 139 on page 1189 summarizes further configuration guidelines for analyzers.

Table 144: Configuration Guidelines for Port Mirroring Analyzers

Guideline	Value or Support Information	Comment
Number of analyzers that you can enable concurrently.	64 Default analyzers 2 per FPC–Statistical analyzer	Statistical analyzers must be bound to an FPC for mirroring traffic on ports belonging to that FPC. **NOTE:** Default analyzer properties are implicitly bound on the last (or second to last) instance on all FPCs in the system. Therefore, when you explicitly bind a second statistical

Table 144: Configuration Guidelines for Port Mirroring Analyzers *(continued)*

Guideline	Value or Support Information	Comment
		analyzer on the FPC, the default analyzer properties are overridden.
Number of interfaces, VLANs, or bridge domains that you can use as ingress input to an analyzer.	256	–
Types of ports on which you cannot mirror traffic.	• Virtual Chassis ports (VCPs) • Management Ethernet ports (me0 or vme0) • Integrated routing and bridging (IRB) interfaces • VLAN-tagged Layer 3 interfaces	
Protocol families that you can include in an analyzer.	**ethernet-switching** for EX Series switches and **bridge** for MX Series routers.	Analyzer mirrors only bridged traffic. To mirror routed traffic, use the port mirroring configuration with **family** as **inet** or **inet6**.
Packets with physical layer errors are not sent to the local or remote analyzer.	Applicable	Packets with these errors are filtered out and thus are not sent to the analyzer.
Analyzer does not support line-rate traffic.	Applicable	Mirroring for line-rate traffic is done on a best-effort basis.
Analyzer output on a LAG interface.	Supported	

Table 144: Configuration Guidelines for Port Mirroring Analyzers *(continued)*

Guideline	Value or Support Information	Comment
Analyzer output interface mode as trunk mode.	Supported	• The trunk interface has to be a member of all VLANs or bridge domains that are related to the input configuration of the analyzer. • You must use the mirror-once option if the input has been configured as VLAN or bridge domain and the output is a trunk interface. **NOTE:** With the mirror-once option, if the analyzer input is from both ingress and egress mirroring, only ingress traffic is mirrored. If both ingress and egress mirroring are required, the output interface cannot be a trunk. In such cases, configure the interface as an access interface.
Egress mirroring of host-generated control packets.	Not supported	
Configuring Layer 3 logical interfaces in the **input** stanza of an analyzer.	Not supported	
The analyzer input and output stanzas containing members of the same VLAN or the VLAN itself must be avoided.	Applicable	
Support for VLAN and its member interfaces in different analyzer sessions	Not supported	If mirroring is configured, either of the analyzers is active.
Egress mirroring of aggregated Ethernet (ae) interfaces and its child logical interfaces configured for different analyzers.	Not supported	

RELATED DOCUMENTATION

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)

IN THIS SECTION

- Configuring an Analyzer for Local Traffic Analysis | 1222
- Configuring an Analyzer for Remote Traffic Analysis | 1223
- Configuring a Statistical Analyzer for Local Traffic Analysis | 1224
- Configuring a Statistical Analyzer for Remote Traffic Analysis | 1225
- Binding Statistical Analyzers to Ports Grouped at the FPC Level | 1226
- Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups | 1227
- Defining a Next-Hop Group for Layer 2 Mirroring | 1228

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy the following packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable the analyzers that you have configured when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
  - Using statistical sampling.
  - Setting ratios to select statistical samples.
  - Using firewall filters.

NOTE: If you want to create additional analyzers without deleting the existing analyzers, disable the existing analyzers by using the **disable analyzer *analyzer-name*** statement from the command-line-interface (CLI) or from the J-Web configuration page for mirroring.

NOTE: Interfaces used as output to an analyzer must be configured under the **ethernet-switching family**, and must be associated to a VLAN.

Configuring an Analyzer for Local Traffic Analysis

To mirror network traffic or VLAN traffic on the switch to an interface on the switch by using analyzers:

1. Choose a name for the analyzer and specify the input:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface interface-name
   ```

   For example, create an analyzer called **employee-monitor** to monitor the packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface ge–0/0/0.0
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
   ```

2. Configure the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output interface interface-name
   ```

   For example, configure ge-0/0/10.0 as the destination interface for the **employee-monitor** analyzer:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

Configuring an Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN used for analysis from a remote location:

1. Configure a VLAN to carry the mirrored traffic:

   ```
   [edit]
   user@switch# set vlans analyzer-name vlan-id vlan-ID
   ```

   For example, define an analyzer VLAN called **remote-analyzer** and assign it the VLAN ID **999**:

   ```
   [edit]
   user@switch# set vlans remote-analyzer vlan-id 999
   ```

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the analyzer VLAN:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode access vlan members vlan-ID
   ```

   For example, set the interface ge-0/1/1 to access mode and associate it with the analyzer VLAN ID **999**:

   ```
   [edit]
   user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode access vlan members 999
   ```

3. Configure the analyzer:

   a. Define an analyzer and specify the traffic to be mirrored:

      ```
      [edit forwarding-options]
      user@switch# set analyzer analyzer-name input ingress interface interface-name
      ```

      For example, define the **employee-monitor** analyzer for which traffic to be mirrored comprises packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

      ```
      [edit forwarding-options]
      user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
      [edit forwarding-options]
      user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
      ```

   b. Specify the analyzer VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output analyzer for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

Configuring a Statistical Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch by using a statistical analyzer:

1. Choose a name for the analyzer and specify the input interfaces:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface interface-name
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
   ```

   For example, specify an analyzer called **employee-monitor** and specify the input interfaces ge-0/0/0 and ge-0/0/1:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface ge–0/0/0.0
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
   ```

2. Configure the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface interface-name
   ```

   For example, configure ge-0/0/10.0 as the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

3. Specify mirroring properties.

   a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

      ```
      [edit forwarding-options]
      ```

```
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

b. Specify at what length mirrored packets are truncated:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, indicating that mirrored packets are not truncated.

Configuring a Statistical Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location by using a statistical analyzer:

1. Configure a VLAN to carry the mirrored traffic:

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

   For example, configure a VLAN called **remote-analyzer** with VLAN ID **999**:

   ```
   [edit]
   user@switch# set vlans remote-analyzer vlan-id 999
   ```

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the VLAN:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode access vlan members vlan-ID
   ```

   For example, set the uplink module interface ge-0/1/1.0 that is connected to the distribution switch to access mode and associate it with the **remote-analyzer** VLAN:

   ```
   [edit]
   user@switch# set interfaces ge-0/1/1.0 unit 0 family ethernet-switching interface-mode access vlan members 999
   ```

3. Configure the statistical analyzer:

   a. Specify the traffic to be mirrored:

   ```
   [edit forwarding-options]
   ```

```
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, specify the packets entering ports ge-0/0/0.0 and ge-0/0/1.0 to be mirrored:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

b. Specify an output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Specify mirroring properties.

a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

b. Specify the length to which mirrored packets are to be truncated:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, which means the mirrored packets are not truncated.

Binding Statistical Analyzers to Ports Grouped at the FPC Level

You can bind a statistical analyzer to a specific FPC in the switch, that is, you can bind the statistical analyzer instance at the FPC level of the switch. The mirroring properties specified in the statistical analyzer are applied to all physical ports associated with all Packet Forwarding Engines on the specified FPC.

To bind a named instance of Layer 2 analyzer to an FPC:

1. Enable configuration of switch chassis properties:

```
[edit]
user@switch# edit chassis
```

2. Enable configuration of an FPC (and its installed PICs):

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

3. Bind a statistical analyzer instance to the FPC:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-1
```

4. (Optional) To bind a second statistical analyzer instance of Layer 2 mirroring to the same FPC, repeat Step 3 and specify a different statistical analyzer name:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-2
```

5. Verify the minimum configuration of the binding:

```
[edit chassis fpc slot-number port-mirror-instance analyzer_name]
user@switch# top
[edit]
user@switch# show chassis
```

```
chassis {
   fpc slot-number { # Bind two statistical analyzers or port mirroring
                     named instances at the FPC level.
   port-mirror-instance stats_analyzer-1;
   port-mirror-instance stats_analyzer-2;
                  }
               }
```

NOTE: On binding a second instance (**stats_analyzer-2** in this example), the mirroring properties of this session, if configured, overrides any default analyzer.

Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups

You can mirror traffic to multiple destinations by configuring next-hop groups as analyzer output. The mirroring of packets to multiple destinations is also known as multipacket port mirroring.

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch (by using analyzers):

1. Choose a name for the analyzer and specify the input:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input ingress interface interface-name
   ```

   For example, create an analyzer called **employee-monitor** for which the input traffic comprises packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/0.0
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
   ```

2. Configure the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output next-hop-group next-hop-group-name
   ```

   For example, configure the next-hop group **nhg** as the destination for the **employee-monitor** analyzer:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output next-hop-group nhg
   ```

Defining a Next-Hop Group for Layer 2 Mirroring

The next-hop group configuration at the **[edit forwarding-options]** configuration level enables you to define a next-hop group name, the type of addresses to be used in the next-hop group, and the logical interfaces that form the multiple destinations to which traffic can be mirrored. By default, the next-hop group is specified using Layer 3 addresses using the **[edit forwarding-options next-hop-group *next-hop-group-name* group-type inet]** statement. To specify a next-hop group using Layer 2 addresses instead, include the **[edit forwarding-options next-hop-group *next-hop-group-name* group-type layer-2]** statement.

To define a next-hop group for Layer 2 mirroring:

1. Enable configuration of a next-hop group for Layer 2 mirroring:

   ```
   [edit forwarding-options ]
   user@switch# set next-hop-group next-hop-group-name
   ```

   For example, configure **next-hop-group** with name **nhg**:

   ```
   [edit forwarding-options]
   ```

```
user@switch# set next-hop-group nhg
```

2. Specify the type of addresses to be used in the next-hop group configuration:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set group-type layer-2
```

For example, configure **next-hop-group type** as **layer-2** because the analyzer output must be **layer-2** only:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg group-type layer-2
```

3. Specify the logical interfaces of the next-hop group:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set interface logical-interface-name-1
user@switch# set interface logical-interface-name-2
```

For example, to specify ge-0/0/10.0 and ge-0/0/11.0 as the logical interfaces of the next-hop group **nhg**:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg interface ge-0/0/10.0
user@switch# set next-hop-group nhg interface ge-0/0/11.0
```

RELATED DOCUMENTATION

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Understanding Port Mirroring Analyzers | **1214**

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure)

IN THIS SECTION

- Configuring an Analyzer for Local Traffic Analysis | 1231
- Configuring an Analyzer for Remote Traffic Analysis | 1231
- Configuring Port Mirroring | 1233

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring configurations when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

NOTE: If you want to create additional analyzers without deleting the existing analyzers, then disable the existing analyzers by using the **disable analyzer *analyzer-name*** statement from the command-line interface or the J-Web configuration page for mirroring.

NOTE: Interfaces used as output for an analyzer must be configured under the **ethernet-switching** family.

Configuring an Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch (by using analyzers):

1. Choose a name for the analyzer and specify the input:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface interface-name
   ```

   For example, create an analyzer called **employee-monitor** for which the input traffic is packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

   ```
   [edit forwarding-options]
   user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface ge–0/0/0.0
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
   ```

2. Configure the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output interface interface-name
   ```

   For example, configure ge-0/0/10.0 as the destination interface for the **employee-monitor** analyzer:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

Configuring an Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location (by using analyzers):

1. Configure a VLAN to carry the mirrored traffic:

   ```
   [edit]
   user@switch# set vlans analyzer-name vlan-id vlan-ID
   ```

   For example, define an analyzer VLAN called **remote-analyzer** and assign it a VLAN ID of **999**:

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Set the uplink module interface that is connected to the distribution switch to trunk mode and associate it with the analyzer VLAN:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode trunk vlan members vlan-ID
   ```

   For example, set the interface ge-0/1/1 to trunk mode and associate it with the analyzer VLAN ID **999**:

   ```
   [edit]
   user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode trunk vlan members 999
   ```

3. Configure the analyzer:

   a. Define an analyzer and specify the traffic to be mirrored:

      ```
      [edit forwarding-options]
      user@switch# set analyzer analyzer-name input ingress interface interface-name
      ```

      For example, define the **employee-monitor** analyzer for which traffic to be mirrored is packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

      ```
      [edit forwarding-options]
      user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
      [edit forwarding-options]
      user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
      ```

   b. Specify the analyzer VLAN as the output for the analyzer:

      ```
      [edit forwarding-options]
      user@switch# set analyzer analyzer-name output vlan vlan-ID
      ```

      For example, specify the **remote-analyzer** VLAN as the output analyzer for the **employee-monitor** analyzer:

      ```
      [edit forwarding-options]
      user@switch# set analyzer employee-monitor output vlan 999
      ```

Configuring Port Mirroring

To filter packets to be mirrored to a port-mirroring instance, create the instance and then use it as the action in the firewall filter. You can use firewall filters in both local and remote mirroring configurations.

If the same port-mirroring instance is used in multiple filters or terms, the packets are copied to the analyzer output port or analyzer VLAN only once.

To filter mirrored traffic, create a port-mirroring instance under the **[edit forwarding-options]** hierarchy level, and then create a firewall filter. The filter can use any of the available match conditions and must have **port-mirror-instance *instance-name*** as an action. This action in the firewall filter configuration provides the input to the port-mirroring instance.

To configure a port-mirroring instance with firewall filters:

1. Configure the port-mirroring instance name (here, **employee-monitor**) and the output:

   a. For local analysis, set the output to the local interface where you will connect the computer running the protocol analyzer:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output interface ge-0/0/10.0
   ```

   b. For remote analysis, set the output to the **remote-analyzer** VLAN:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output vlan 999
   ```

2. Create a firewall filter by using any of the available match conditions and assign **employee-monitor** to the **port-mirror-instance** action:

   This step shows a firewall filter **example-filter**, with two terms (**no-analyzer** and **to-analyzer**):

   a. Create the first term to define the traffic that should not pass through to the port-mirroring instance **employee-monitor**:

   ```
   [edit firewall family ethernet-switching
   user@switch# set filter example-filter term no-analyzer from source-address ip-address
   user@switch# set filter example-filter term no-analyzer from destination-address ip-address
   user@switch# set filter example-filter term no-analyzer then accept
   ```

   b. Create the second term to define the traffic that should pass through to the port-mirroring instance **employee-monitor**:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
user@switch# set filter example-filter term to-analyzer then port-mirror-instance employee–monitor
user@switch# set filter example-filter term to-analyzer then accept
```

3. Apply the firewall filter to the interfaces or VLAN that provide input to the port-mirroring instance:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input example-filter
ser@switch# set vlan remote-analyzer filter input example-filter
```

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

Firewall Filters for EX Series Switches Overview

Configuring Port Mirroring to Analyze Traffic (CLI Procedure)

IN THIS SECTION

- Configuring Port Mirroring for Local Traffic Analysis | **1235**
- Configuring Port Mirroring for Remote Traffic Analysis | **1236**
- Filtering the Traffic Entering an Analyzer | **1237**

This configuration task uses Junos OS for EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style.

EX Series switches allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use port mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX2200, EX3200, EX3300, EX4200, EX4500, or EX6200 switches

- Packets exiting a VLAN on EX8200 switches

> **BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you:
>
> - Disable your configured port mirroring analyzers when you are not using them.
> - Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
> - Limit the amount of mirrored traffic by:
>   - Using statistical sampling.
>   - Setting ratios to select statistical samples.
>   - Using firewall filters.

Before you begin to configure port mirroring, note the following limitations for analyzer output interfaces:

- Cannot also be a source port.
- Cannot be used for switching.
- Do not participate in Layer 2 protocols (such as RSTP) when part of a port mirroring configuration.
- Do not retain any VLAN associations they held before they were configured as analyzer output interfaces.

> **NOTE:** If you want to create additional analyzers without deleting the existing analyzer, first disable the existing analyzer using the **disable analyzer *analyzer-name*** command or the J-Web configuration page for port mirroring.

> **NOTE:** Interfaces used as output for an analyzer must be configured as family **ethernet-switching**.

Configuring Port Mirroring for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to another interface on the switch:

1. Choose a name for the analyzer—in this case **employee-monitor**—and specify the input—in this case, packets entering **ge-0/0/0** and **ge-0/0/1**:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ingress interface ge–0/0/0.0
[edit ethernet-switching-options]
```

```
user@switch# set analyzer employee-monitor input ingress interface ge–0/0/1.0
```

2. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor ratio 200
   ```

   When the ratio is set to 200, 1 of every 200 packets is mirrored to the analyzer. You can use statistical sampling to reduce the volume of mirrored traffic, as a high volume of mirrored traffic can be performance intensive for the switch. On EX8200 switches, you can set a ratio only for ingress packets.

3. Configure the destination interface for the mirrored packets:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

Configuring Port Mirroring for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location:

1. Configure a VLAN to carry the mirrored traffic. This VLAN is called **remote-analyzer** and given the ID of 999 by convention in this documentation:

   ```
   [edit]
   user@switch# set vlans remote-analyzer vlan-id 999
   ```

2. Set the uplink module interface that is connected to the distribution switch to trunk mode and associate it with the **remote-analyzer** VLAN:

   ```
   [edit]
   user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching port-mode trunk vlan members 999
   ```

3. Configure the analyzer:

   a. Choose a name and set the loss priority to high. Loss priority should always be set to high when configuring for remote port mirroring:

      ```
      [edit ethernet-switching-options]
      user@switch# set analyzer employee-monitor loss-priority high
      ```

   b. Specify the traffic to be mirrored—in this example the packets entering ports **ge-0/0/0** and **ge-0/0/1**:

      ```
      [edit ethernet-switching-options]
      ```

```
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

c. Specify the **remote-analyzer** VLAN as the output for the analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

When the ratio is set to 200, 1 out of every 200 packets is mirrored to the analyzer. You can use this to reduce the volume of mirrored traffic as a very high volume of mirrored traffic can be performance intensive for the switch.

Filtering the Traffic Entering an Analyzer

To filter which packets are mirrored to an analyzer, create the analyzer and then use it as the action in the firewall filter. You can use firewall filters in both local and remote port mirroring configurations.

If the same analyzer is used in multiple filters or terms, the packets are copied to the analyzer output port or analyzer VLAN only once.

To filter mirrored traffic, create an analyzer and then create a firewall filter. The filter can use any of the available match conditions and must have an action of **analyzer**. The action of the firewall filter provides the input to the analyzer.

To configure port mirroring with filters:

1. Configure the analyzer name (here, **employee-monitor**) and the output:

a. For local analysis, set the output to the local interface to which you will connect the computer running the protocol analyzer application:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

b. For remote analysis, set the loss priority to high and set the output to the **remote-analyzer** VLAN:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor loss-priority high output vlan 999
```

2. Create a firewall filter using any of the available match conditions and specify the action as **analyzer**:

This step shows a firewall filter called **example-filter**, with two terms:

a. Create the first term to define the traffic that should not pass through to the analyzer:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from source-address ip-address
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from destination-address ip-address
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer then accept
```

b. Create the second term to define the traffic that should pass through to the analyzer:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then analyzer employee–monitor
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then accept
```

3. Apply the firewall filter to the interfaces or VLAN that are input to the analyzer:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input example-filter
[edit]
user@switch# set vlan remote-analyzer filter input example-filter
```

RELATED DOCUMENTATION

- *Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches*
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches | **1191**

Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches

Purpose

This verification task uses Junos OS for EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style.

Verify that an analyzer has been created on the switch and has the appropriate mirror input interfaces, and the appropriate analyzer output interface.

Action

You can verify the port mirror analyzer is configured as expected by using the **show analyzer** command.

```
[edit]
user@switch>  show analyzer
```

```
Analyzer name                  : employee-monitor
  Output VLAN                  : remote-analyzer
  Mirror ratio                 : 1
  Loss priority                : High
  Ingress monitored interfaces : ge-0/0/0.0
  Ingress monitored interfaces : ge-0/0/1.0
```

You can view all of the port mirror analyzers configured on the switch, including any that are disabled, by using the **show ethernet-switching-options** command in configuration mode.

```
user@switch# show ethernet-switching-options
```

```
inactive: analyzer employee-web-monitor {
    loss-priority high;
    output {

analyzer employee-monitor {
    loss-priority high;
    input {
        ingress {
            interface ge-0/0/0.0;
            interface ge-0/0/1.0;
        }
    }
    output {
        vlan {
            remote-analyzer;
        }
    }
}
```

Meaning

This output shows that the employee-monitor analyzer has a ratio of 1 (mirroring every packet, the default), a loss priority of **high** (set this option to **high** whenever the analyzer output is to a VLAN), is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and is sending the mirrored traffic to the analyzer called remote-analyzer.

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use

IN THIS SECTION

- Requirements | **1241**
- Overview and Topology | **1241**
- Mirroring All Employee Traffic for Local Analysis | **1242**
- Verification | **1244**

Juniper Networks devices allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring, to a VLAN or to a bridge domain for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN or bridge domain

You can then analyze the mirrored traffic locally or remotely using a protocol analyzer. You can install an analyzer on a local destination interface. If you are sending mirrored traffic to an analyzer VLAN or bridge domain, you can use an analyzer on a remote monitoring station.

This topic describes how to configure local mirroring on a switching device. The examples in this topic describe how to configure a switching device to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on that same device.

Requirements

Use either one of the following hardware and software components:

- One EX9200 switch with Junos OS Release 13.2 or later
- One MX Series router with Junos OS Release 14.1 or later

Before you configure port mirroring, be sure you have an understanding of mirroring concepts. For information about analyzers, see "Understanding Port Mirroring Analyzers" on page 1214. For information about port mirroring, see "Understanding Layer 2 Port Mirroring" on page 1200.

Overview and Topology

This topic describes how to mirror all traffic entering ports on the switching device to a destination interface on the same device (local mirroring). In this case, the traffic is entering ports connected to employee computers.

> **NOTE:** Mirroring all traffic requires significant bandwidth and should only be done during an active investigation.

The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers.

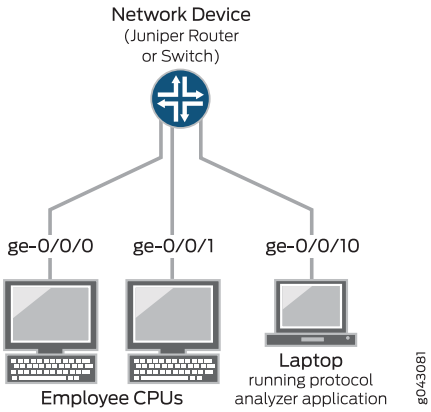
The interface ge-0/0/10 is reserved for analysis of the mirrored traffic.

Connect a PC running a protocol analyzer to the analyzer output interface.

> **NOTE:** Multiple ports mirrored to one interface can cause buffer overflow, resulting in mirrored packets being dropped at the output interface.

Figure 44 on page 1242 shows the network topology for this example.

Figure 44: Network Topology for Local Port Mirroring Example



Mirroring All Employee Traffic for Local Analysis

CLI Quick Configuration

To quickly configure local mirroring for ingress traffic sent on two ports connected to employee computers, copy either of the following commands for EX Series switches or for MX Series routers and paste them into the switching device terminal window:

EX Series

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family ethernet-switching
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

MX Series

```
[edit]
set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99
set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

Step-by-Step Procedure

To configure an analyzer called **employee-monitor** and specify both the input (source) interfaces and the analyzer output interface:

1. Configure each interface to be used in the analyzer configuration. Use the family protocol that is correct for your platform.

   EX Series

   ```
   [edit]
   set interfaces ge-0/0/0 unit 0 family ethernet-switching
   set interfaces ge-0/0/1 unit 0 family ethernet-switching
   ```

   MX Series

   To configure **family bridge** on an interface, you must configure **interface-mode access** or **interface-mode trunk** as well. You also must configure **vlan-id**.

   ```
   [edit]
   set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99
   set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98
   ```

2. Configure each interface connected to employee computers as an output analyzer interface **employee-monitor**.

   ```
   [edit forwarding-options]
   set analyzer employee-monitor input ingress interface ge-0/0/0.0
   set analyzer employee-monitor input ingress interface ge-0/0/1.0
   ```

3. Configure the output analyzer interface for the **employee-monitor** analyzer.

   This will be the destination interface for the mirrored packets.

   ```
   [edit forwarding-options]
   set analyzer employee-monitor output interface ge-0/0/10.0
   ```

Results

Check the results of the configuration.

```
[edit]
user@device# show forwarding-options
```

```
analyzer {
    employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            interface ge-0/0/10.0;
        }
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer **employee-monitor** has been created on the switching device with the appropriate input interfaces and the appropriate output interface.

Action

Use the **show forwarding-options analyzer** operational command to verify that an analyzer is configured as expected.

`user@device>` **show forwarding-options analyzer**

```
Analyzer name                    : employee-monitor
  Mirror rate                      : 1
  Maximum packet length            : 0
  State                            : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Output interface                 : ge-0/0/10.0
```

Meaning

The output shows that the **employee-monitor** analyzer has a ratio of 1 (that is, mirroring every packet, the default setting), the maximum size of the original packet mirrored is 0 (indicating that the entire packet is mirrored), the state of the configuration is **up**, and the analyzer is mirroring the traffic entering the ge-0/0/0 interface, and sending the mirrored traffic to the ge-0/0/10 interface.

If the state of the output interface is **down** or if the output interface is not configured, the value of **State** will be **down** indicating that the analyzer will not be receiving mirrored traffic.

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**

Understanding Port Mirroring Analyzers | **1214**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use

IN THIS SECTION

- Requirements | **1246**
- Overview and Topology | **1246**
- Mirroring Employee Traffic for Remote Analysis By Using a Statistical Analyzer | **1247**
- Verification | **1257**

Juniper Networks devices allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN or bridge domain for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN
- Packets entering or exiting a bridge domain

If you are sending mirrored traffic to an analyzer VLAN or bridge domain, you can analyze the mirrored traffic by using a protocol analyzer running on a remote monitoring station.

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you do the following:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
  - Using statistical sampling.
  - Setting ratios to select statistical samples.
  - Using firewall filters.

The examples in this topic describe how to configure remote port mirroring to analyze employee resource usage.

Requirements

This example uses one of the following pairs of hardware and software components:

- One EX9200 switch connected to another EX9200 switch, both running Junos OS Release 13.2 or later
- One MX Series router connected to another MX Series router, both running Junos OS Release 14.1 or later

Before you configure remote mirroring, be sure that:

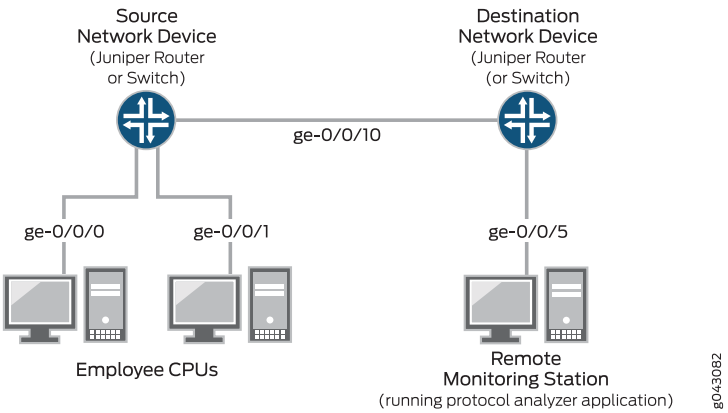
- You have an understanding of mirroring concepts. For information about analyzers, see "Understanding Port Mirroring Analyzers" on page 1214. For information about port mirroring, see "Understanding Layer 2 Port Mirroring" on page 1200.
- The interfaces that the analyzer will use as input interfaces have already been configured on the switching device.

Overview and Topology

This topic describes how to configure port mirroring to a remote analyzer VLAN or bridge domain so that the analysis can be done from a remote monitoring station.

Figure 45 on page 1247 shows the network topology for both the EX Series example and the MX Series example scenarios.

Figure 45: Network Topology for Remote Port Mirroring and Analysis



In this example:

- Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both are interfaces on the source device) that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects the source switching device to the destination switching device.
- Interface ge-0/0/5 is a Layer 2 interface that connects the destination switching device to the remote monitoring station.
- The analyzer **remote-analyzer** is configured on all switching devices in the topology to carry the mirrored traffic. This topology can use either a VLAN or a bridge domain.

Mirroring Employee Traffic for Remote Analysis By Using a Statistical Analyzer

IN THIS SECTION

- Mirroring Employee Traffic for Remote Analysis for EX Series Switches | **1247**
- Mirroring Employee Traffic for Remote Analysis for MX Series Routers | **1252**

To configure a statistical analyzer for remote traffic analysis for all incoming and outgoing employee traffic, select one of the following examples:

Mirroring Employee Traffic for Remote Analysis for EX Series Switches

CLI Quick Configuration

To quickly configure a statistical analyzer for remote traffic analysis of the incoming and outgoing employee traffic, copy the following commands for EX Series switches and paste them into the correct switching device terminal window.

- Copy and paste the following commands in the *source* switching device terminal window:

  EX Series

  ```
  [edit]
  set vlans remote-analyzer vlan-id 999
  set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
  set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
  set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
  set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
  set forwarding-options analyzer employee-monitor output vlan remote-analyzer
  set forwarding-options analyzer employee-monitor input rate 2
  set forwarding-options analyzer employee-monitor input maximum-packet-length 128
  set chassis fpc 0 port-mirror-instance employee-monitor
  ```

- Copy and paste the following commands in the *destination* switching device terminal window:

  EX Series

  ```
  [edit]
  set vlans remote-analyzer vlan-id 999
  set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
  set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
  set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode access
  set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
  set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
  ```

Step-by-Step Procedure

To configure basic remote mirroring:

1. On the source switching device, do the following:

   - Configure the VLAN ID for the **remote-analyzer** VLAN.

     ```
     [edit]
     user@device# set vlans remote-analyzer vlan-id 999
     ```

   - Configure the interface on the network port connected to the destination switching device for access mode and associate it with the **remote-analyzer** VLAN.

```
[edit]
user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the statistical analyzer **employee-monitor**.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@device# set analyzer employee-monitor output vlan remote-analyzer
user@device# set analyzer employee-monitor input rate 2
user@device# set analyzer employee-monitor input maximum-packet-length 128
```

- Bind the statistical analyzer to the FPC that contains the input interface.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

2. On the destination network device, do the following:

   - Configure the VLAN ID for the **remote-analyzer** VLAN.

```
[edit]
user@device# set vlans remote-analyzer vlan-id 999
```

   - Configure the interface on the destination switching device for access mode and associate it with the **remote-analyzer** VLAN.

```
[edit interfaces]
user@device# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@device# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

   - Configure the interface connected to the destination switching device for access mode.

```
[edit interfaces]
user@device# set ge-0/0/5 unit 0 family ethernet-switching interface-mode access
```

   - Configure the **employee-monitor** analyzer.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress vlan remote-analyzer
```

```
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Specify mirroring parameters such as rate and the maximum packet length for the **employee-monitor** analyzer.

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input maximum-packet-length 128
```

- Bind the **employee-monitor** analyzer to the FPC containing the input ports.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

Results

Check the results of the configuration on the source switching device:

```
[edit]
user@device# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            maximum-packet-length 128;
            rate 2;
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
interfaces {
    ge-0/0/10 {
```

```
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Check the results of the configuration on the destination switching device.

```
[edit]
user@device# show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0;
```

```
        }
      }
    }
    forwarding-options {
      analyzer employee-monitor {
        input {
          ingress {
            vlan remote-analyzer;
          }
        }
        output {
          interface {
            ge-0/0/5.0;
          }
        }
      }
    }
```

Mirroring Employee Traffic for Remote Analysis for MX Series Routers

CLI Quick Configuration

To quickly configure a statistical analyzer for remote traffic analysis of incoming and outgoing employee traffic, copy the following commands for MX Series routers and paste them into the correct switching device terminal window.

- Copy and paste the following commands in the *source* switching device terminal window:

  MX Series

  ```
  [edit]
  set bridge-domains remote-analyzer vlan-id 999
  set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
  set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
  set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
  set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
  set forwarding-options analyzer employee-monitor output bridge-domain remote-analyzer
  set forwarding-options analyzer employee-monitor input rate 2
  set forwarding-options analyzer employee-monitor input maximum-packet-length 128
  set chassis fpc 0 port-mirror-instance employee-monitor
  ```

- Copy and paste the following commands in the *destination* switching device terminal window:

MX Series

```
[edit]
set bridge-domains remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
set interfaces ge-0/0/5 unit 0 family bridge interface-mode access
set forwarding-options analyzer employee-monitor input ingress bridge-domain remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

Step-by-Step Procedure

To configure basic remote mirroring using MX Series routers:

1. On the source switching device, do the following:
   - Configure the VLAN ID for the **remote-analyzer** bridge domain.

     ```
     [edit]
     user@device# set bridge-domains remote-analyzer vlan-id 999
     ```

   - Configure the interface on the network port connected to the destination switching device for access mode and associate it with the **remote-analyzer** bridge domain.

     ```
     [edit]
     user@device# set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
     user@device# set interfaces ge-0/0/10 unit 0 family bridge vlan members 999
     ```

   - Configure the statistical analyzer **employee-monitor**.

     ```
     [edit forwarding-options]
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor output bridge-domain remote-analyzer
     user@device# set analyzer employee-monitor input rate 2
     user@device# set analyzer employee-monitor input maximum-packet-length 128
     ```

   - Bind the statistical analyzer to the FPC that contains the input interface.

     ```
     [edit]
     user@device# set chassis fpc 0 port-mirror-instance employee-monitor
     ```

2. On the destination switching device, do the following:

- Configure the VLAN ID for the **remote-analyzer** bridge domain.

```
[edit bridge-domains]
user@device# set remote-analyzer vlan-id 999
```

- Configure the interface on the destination switching device for access mode and associate it with the **remote-analyzer** bridge domain.

```
[edit interfaces]
user@device# set ge-0/0/10 unit 0 family bridge interface-mode access
user@device# set ge-0/0/10 unit 0 family bridge vlan members 999
```

- Configure the interface connected to the destination switching device for access mode.

```
[edit interfaces]
user@device# set ge-0/0/5 unit 0 family bridge interface-mode access
```

- Configure the **employee-monitor** analyzer.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress bridge-domain remote-analyzer
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Specify mirroring parameters such as rate and the maximum packet length for the **employee-monitor** analyzer.

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input maximum-packet-length 128
```

- Bind the **employee-monitor** analyzer to the FPC containing the input ports.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

Results

Check the results of the configuration on the source switching device:

```
[edit]
user@device# show
bridge-domains {
```

```
    remote-analyzer {
        vlan-id 999;
    }
}
forwarding-options {
    analyzer {
        employee-monitor {
            input {
                ingress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                }
                egress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                }
                maximum-packet-length 128;
                rate 2;
            }
            output {
                bridge-domain {
                    remote-analyzer;
                }
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 99;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 98;
            }
        }
    }
```

```
    ge-0/0/10 {
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 999;
            }
        }
    }
}
```

Check the results of the configuration on the destination switching device.

```
[edit]
user@device# show
bridge-domains {
    remote-analyzer {
        vlan-id 999;
    }
}
forwarding-options {
    analyzer {
        employee-monitor {
            input {
                ingress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                    bridge-domain remote-analyzer;
                }
            }
            output {
                interface ge-0/0/5.0;
            }
        }
    }
}
interfaces {
    ge-0/0/5 {
        unit 0 {
            family bridge {
                interface-mode access;
            }
        }
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** has been created on the device with the appropriate input interfaces and the appropriate output interface.

Action

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switching device, run the **show forwarding-options analyzer** command on the source switching device. The following output is displayed for this configuration example.

```
user@device> show forwarding-options analyzer
```

```
Analyzer name                    : employee-monitor
  Mirror rate                      : 2
  Maximum packet length            : 128
  State                            : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces      : ge-0/0/0.0
  Egress monitored interfaces      : ge-0/0/1.0
  Output VLAN                      : default-switch/remote-analyzer
```

Meaning

This output shows that the **employee-monitor** instance has a ratio of 2, the maximum size of the original packet that were mirrored is 128, the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, and the analyzer is mirroring the traffic entering ge-0/0/0.0 and ge-0/0/1.0, and is sending the mirrored traffic to the VLAN called remote-analyzer.

If the state of the output interface is **down** or if the output interface is not configured, the value of **State** will be down and the analyzer will not be able to monitor traffic.

RELATED DOCUMENTATION

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**

Understanding Port Mirroring Analyzers | 1214

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches

IN THIS SECTION

- Requirements | 1259
- Overview and Topology | 1259
- Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis | 1261
- Verification | 1267

EX9200 switches allow you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN on

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring analyzers when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
  - Using statistical sampling.
  - Setting ratios to select statistical samples.
  - Using firewall filters.

This example describes how to configure remote mirroring to multiple interfaces on an analyzer VLAN:

Requirements

This example uses the following hardware and software components:

- Three EX9200 switches
- Junos OS Release 13.2 or later for EX Series switches

Before you configure remote mirroring, be sure that:

- You have an understanding of mirroring concepts. For information about analyzers, see "Understanding Port Mirroring Analyzers" on page 1214. For information about port mirroring, see "Understanding Layer 2 Port Mirroring" on page 1200.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

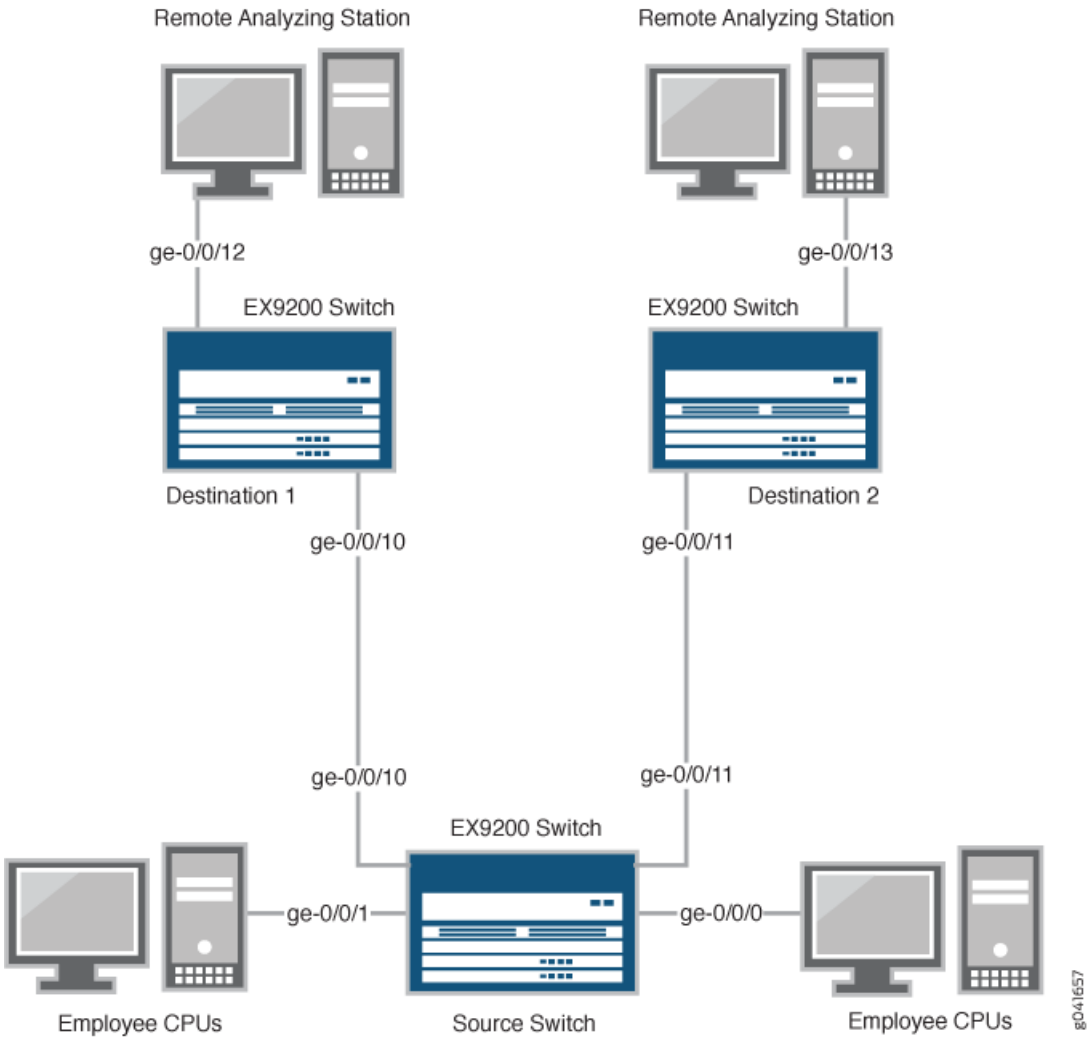
Overview and Topology

This example describes how to mirror traffic entering ports on the switch to the remote analyzer VLAN so that you can perform analysis from a remote monitoring station. The remote-analyzer VLAN in this example contains multiple member interfaces. Therefore, the same traffic is mirrored to all member interfaces of the remote-analyzer VLAN so that mirrored packets can be sent to different remote monitoring stations. You can install applications, such as sniffers and intrusion detection systems, on remote monitoring stations to analyze these mirrored packets and to obtain useful statistical data. For instance, if there are two remote monitoring stations, you can install a sniffer on one remote monitoring station and an intrusion detection system on the other station. You can use a firewall filter analyzer configuration to forward a specific type of traffic to a remote monitoring station.

This example describes how to configure an analyzer to mirror traffic to multiple interfaces in the next-hop group so that traffic is sent to different monitoring stations for analysis.

Figure 46 on page 1260 shows the network topology for this example.

Figure 46: Remote Mirroring Example Network Topology Using Multiple VLAN Member Interfaces in the Next-Hop Group



In this example:

- Interfaces ge-0/0/0 and ge-0/0/1 are Layer 2 interfaces (both interfaces on the source switch) that serve as connections for employee computers.
- Interfaces ge-0/0/10 and ge-0/0/11 are Layer 2 interfaces that are connected to different destination switches.
- Interface ge-0/0/12 is a Layer 2 interface that connects the Destination 1 switch to the remote monitoring station.
- Interface ge-0/0/13 is a Layer 2 interface that connects the Destination 2 switch to the remote monitoring station.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis

To configure mirroring to multiple VLAN member interfaces for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure mirroring for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- In the source switch terminal window, copy and paste the following commands:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output next-hop-group remote-analyzer-nhg
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
set forwarding-options next-hop-group remote-analyzer-nhg group-type layer-2
```

- In the Destination 1 switch terminal window, copy and paste the following commands:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode acess
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor loss-priority high output interface ge-0/0/12.0
```

- In the Destination 2 switch terminal window, copy and paste the following commands:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode access
```

set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer

set forwarding-options analyzer employee-monitor loss-priority high output interface ge-0/0/13.0

Step-by-Step Procedure

To configure basic remote mirroring to two VLAN member interfaces:

1. On the source switch:

   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure the interfaces on the network port connected to destination switches for access mode and associate it with the **remote-analyzer** VLAN:

     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/11 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure the **employee-monitor** analyzer:

     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor output next-hop-group remote-analyzer-nhg
     ```

     In this analyzer configuration, traffic that enters and exits interfaces ge-0/0/0.0 and ge-0/0/1.0 are sent to the output destination defined by the next-hop group named **remote-analyzer-nhg**.

   - Configure the **remote-analyzer-nhb** next-hop group:

     ```
     [edit forwarding-options]
     user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
     user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
     user@switch# set next-hop-group remote-analyzer-nhg group-type layer-2
     ```

2. On the Destination 1 switch:

   - Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the ge-0/0/10 interface on the Destination 1 switch for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
```

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface ge-0/0/12.0
```

3. On the Destination 2 switch:

- Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the ge-0/0/11 interface on the Destination 2 switch for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface ge-0/0/13.0
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            next-hop-group {
                remote-analyzer-nhg;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            ge-0/0/11.0
        }
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
```

```
    }
}
```

Check the results of the configuration on the Destination 1 switch:

```
[edit]
user@switch# show
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            ethernet-switching {
                interface-mode acess;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
            interface-mode access;
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
            vlan remote-analyzer;
            }
        }
        loss-priority high;
        output {
            interface {
                ge-0/0/12.0;
            }
        }
    }
}
```

Check the results of the configuration on the Destination 2 switch:

```
[edit]
user@switch# show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0
        }
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
        family ethernet-switching {
            interface-mode access;
        }
        }
    }
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
}
forwarding-options {
    employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        loss-priority high;
        output {
            interface {
                ge-0/0/13.0;
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying That the Analyzer Has Been Correctly Created | 1267

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify the analyzer is configured as expected by using the **show forwarding-options analyzer** command.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the **show forwarding-options analyzer** command on the source switch. The following output is displayed for this example configuration on the source switch:

```
user@switch> show forwarding-options analyzer
```

```
  Analyzer name                    : employee-monitor
  Mirror rate                       : 1
  Maximum packet length            : 0
  State                             : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces     : ge-0/0/0.0
  Egress monitored interfaces     : ge-0/0/1.0
  Output nhg                        : remote-analyzer-nhg
```

```
user@switch> show forwarding-options next-hop-group
```

```
Next-hop-group: remote-analyzer-nhg
  Type:  layer-2
  State: up
  Members Interfaces:
```

```
    ge-0/0/10.0
    ge-0/0/11.0
```

Meaning

This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, which is the default behavior), the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, mirrors traffic entering or exiting interfaces ge-0/0/0 and ge-0/0/1, and sends mirrored traffic to multiple interfaces ge-0/0/10.0 and ge-0/0/11.0 through the next-hop-group **remote-analyzer-nhg**. If the state of the output interface is **down** or if the output interface is not configured, the value of state will be down and the analyzer will not be able to mirror traffic.

RELATED DOCUMENTATION

- Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | **1268**
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**
- Understanding Port Mirroring Analyzers | **1214**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches

IN THIS SECTION

- Requirements | **1269**
- Overview and Topology | **1269**
- Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch | **1270**
- Verification | **1276**

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes an example that describes how to mirror traffic entering ports on the switch to the remote-analyzer VLAN through a transit switch, so that you can perform analysis from a remote monitoring station.

> **BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you:
>
> - Disable your configured mirroring sessions when you are not using them.
> - Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
> - Limit the amount of mirrored traffic by:
>   - Using statistical sampling.
>   - Setting ratios to select statistical samples.
>   - Using firewall filters.

This example describes how to configure remote mirroring through a transit switch:

Requirements

This example uses the following hardware and software components:

- An EX9200 switch connected to another EX9200 switch through a third EX9200 switch
- Junos OS Release 13.2 or later for EX Series switches

Before you configure remote mirroring, be sure that:

- You have an understanding of mirroring concepts. For information about analyzers, see "Understanding Port Mirroring Analyzers" on page 1214. For information about port mirroring, see "Understanding Layer 2 Port Mirroring" on page 1200.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

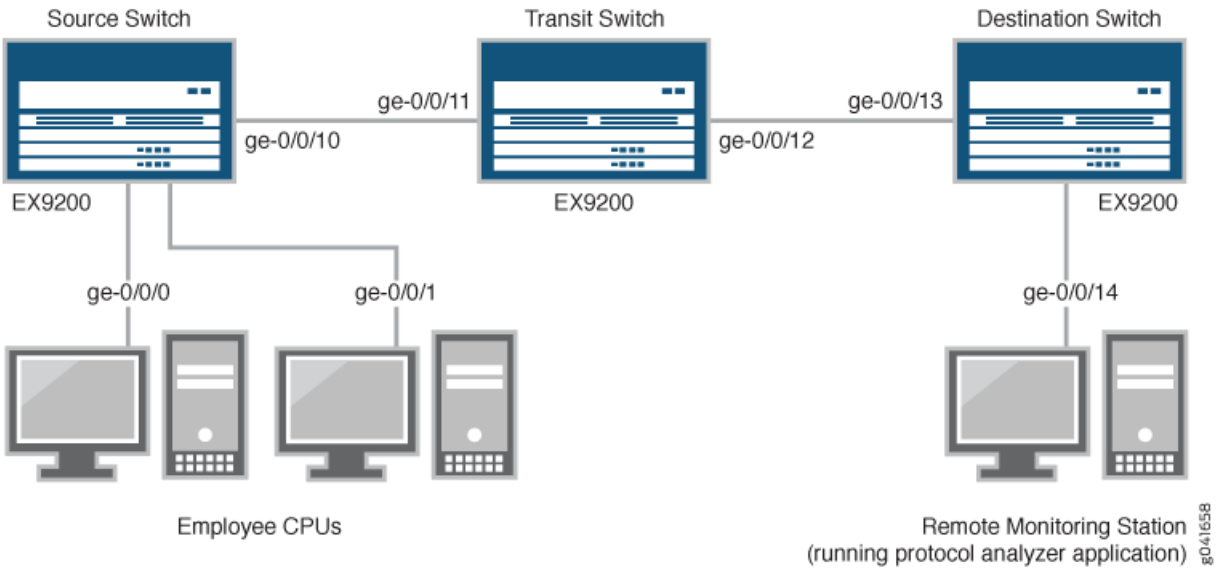
Overview and Topology

This example describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN through a transit switch so that you can perform analysis on all traffic from employee computers.

In this configuration, an analyzer session is required on the destination switch to mirror incoming traffic from the analyzer VLAN to the egress interface to which the remote monitoring station is connected.

Figure 47 on page 1270 shows the network topology for this example.

Figure 47: Network Monitoring for Remote Mirroring Through a Transit Switch



In this example:

a. Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source switch) that serve as connections for employee computers.

b. Interface ge-0/0/10 is a Layer 2 interface that connects to the transit switch.

c. Interface ge-0/0/11 is a Layer 2 interface on the transit switch.

d. Interface ge-0/0/12 is a Layer 2 interface on the transit switch and connects to the destination switch.

e. Interface ge-0/0/13 is a Layer 2 interface on the destination switch.

f. Interface ge-0/0/14 is a Layer 2 interface on the destination switch and connects to the remote monitoring station.

g. VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch

To configure mirroring for remote traffic analysis through a transit switch, for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure mirroring for remote traffic analysis through a transit switch, for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch (monitored switch) terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

- Copy and paste the following commands in the transit switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/11
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/12
```

- Copy and paste the following commands in the destination switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/13 ingress
set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/14.0
```

Step-by-Step Procedure

To configure remote mirroring through a transit switch:

1. On the source switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     ```

```
user@switch# set remote-analyzer vlan-id 999
```

- Configure the interfaces on the network port connected to transit switch for access mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. On the transit switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure the ge-0/0/11 interface for access mode, associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

   - Configure the ge-0/0/12 interface for access mode, associate it with the **remote-analyzer** VLAN, and set the interface for egress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/12
```

3. On the destination switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure the ge-0/0/13 interface for access mode, associate it with the **remote-analyzer** VLAN, and set the interface for ingress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode access
```

- Configure the **remote-analyzer** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
```

```
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    member 999;
                }
            }
        }
    }
}
```

Check the results of the configuration on the transit switch:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0 {
            }
            ge-0/0/12.0 {
            }
        }
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
```

```
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/13.0 {
                ingress;
            }
        }
    }
}
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/14.0;
            }
        }
```

```
    }
  }
```

Verification

IN THIS SECTION

- Verifying That the Analyzer Has Been Correctly Created | 1276

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** has been created on the switch with the appropriate input interfaces and the appropriate output interface.

Action

You can verify the analyzer is configured as expected by using the **show forwarding-options analyzer** command.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the **show forwarding-options analyzer** command on the source switch. The following output is displayed for this example configuration:

`user@switch>` **show forwarding-options analyzer**

```
Analyzer name                    : employee-monitor
  Mirror rate                      : 1
  Maximum packet length            : 0
  State                            : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces      : ge-0/0/0.0
  Egress monitored interfaces      : ge-0/0/1.0
  Output vlan                      : default-switch/remote-analyzer
```

Meaning

This output shows that the **employee-monitor** analyzer has a mirroring ratio of 1 (mirroring every packet, the default), the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and is sending the mirrored traffic to the analyzer called **remote-analyzer**. If the state of the output interface is **down** or if the output interface is not configured, the value of state will be down and the analyzer will not be able to mirror traffic.

RELATED DOCUMENTATION

- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**
- Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**
- Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) | **1221**
- Understanding Port Mirroring Analyzers | **1214**

Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches

IN THIS SECTION

- Requirements | **1278**
- Overview and Topology | **1278**
- Mirroring All Employee Traffic for Local Analysis | **1279**
- Mirroring Employee-to-Web Traffic for Local Analysis | **1281**
- Verification | **1284**

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN

You can analyze the mirrored traffic by using a protocol analyzer installed on a system connected to the local destination interface or a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This example describes how to configure local mirroring on an EX4300 switch. This example describes how to configure the switch to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on the same switch.

Requirements

This example uses the following hardware and software components:

- One EX4300 switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure mirroring, be sure you have an understanding of mirroring concepts.

Overview and Topology

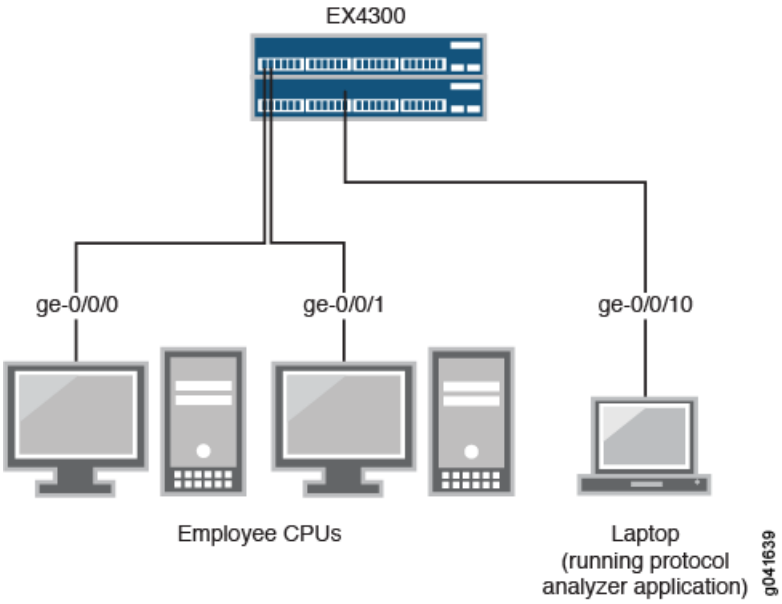
This topic includes two examples that describe how to mirror traffic entering ports on the switch to a destination interface on the same switch (local mirroring). The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario, but includes a filter to mirror only the employee traffic going to the Web.

The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers. The interface ge0/0/10 is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.

NOTE: Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

Both examples use the network topology shown in Figure 44 on page 1242.

Figure 48: Network Topology for Local Mirroring Example



Mirroring All Employee Traffic for Local Analysis

IN THIS SECTION

- [xref target has no title]

To configure mirroring for all employee traffic for local analysis, perform these tasks:

CLI Quick Configuration

To quickly configure local mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members analyzer_vlan
set vlans analyzer-vlan vlan-id 1000
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

Step-by-Step Procedure

To configure an analyzer called **employee-monitor** and specify the input (source) interfaces and the analyzer output interface:

1. Configure each interface connected to employee computers as an input interface for the analyzer **employee-monitor**:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge–0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the output interface of the analyzer as part of a VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members analyzer_vlan
```

```
[edit vlans]
user@switch# set analyzer-vlan vlan-id 1000
```

3. Configure the output analyzer interface for the analyzer **employee-monitor**. This will be the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
            interface ge-0/0/1.0;}
        }
        output {
            interface {
                ge-0/0/10.0;
```

```
        }
      }
    }
}
```

Mirroring Employee-to-Web Traffic for Local Analysis

IN THIS SECTION

- [xref target has no title]

To configure mirroring for employee to Web traffic, perform these tasks:

CLI Quick Configuration

To quickly configure local mirroring of traffic from the two ports connected to employee computers, filtering so that only traffic to the external Web is mirrored, copy the following commands and paste them into the switch terminal window:

```
[edit]
set forwarding-options port-mirroring instance employee-web-monitor output interface ge-0/0/10.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from destination-address
    192.0.2.16/24
set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-address
    192.0.2.16/24
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirroring-instance
    employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

To configure local mirroring of employee to Web traffic from the two ports connected to employee computers:

1. Configure the local analyzer interface:

   ```
   [edit interfaces]
   ```

```
user@switch# set ge-0/0/10 unit 0 family ethernet-switching
```

2. Configure the **employee-web-monitor** output instance (the input to the instance comes from the action of the filter):

```
[edit forwarding-options port-mirroring]
user@switch# set instance employee-web-monitor output interface ge-0/0/10.0
```

3. Configure a firewall filter called **watch-employee** to send mirrored copies of employee requests to the Web to the **employee-web-monitor** instance. Accept all traffic to and from the corporate subnet (destination or source address of 192.0.2.16/24). Send mirrored copies of all packets destined for the Internet (destination port 80) to the **employee-web-monitor** instance.

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address 192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp then accept
ser@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirroring-instance
   employee-web-monitor
```

4. Apply the **watch-employee** filter to the appropriate ports:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
   port-mirroring {
      instance {
         employee-web-monitor {
            family ethernet-switching {
               output {
                  interface ge-0/0/10.0;
```

```
                }
            }
        }
    }
}
...
firewall family ethernet-switching {
    filter watch-employee {
        term employee-to-corp {
            from {
                destination-address 192.0.2.16/24;
                source-address 192.0.2.16/24;
            }
            then accept {
        }
        term employee-to-web {
            from {
                destination-port 80;
            }
            then port-mirroring-instance employee-web-monitor;
        }
    }
}
...
interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan members [employee-vlan, voice-vlan];
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
```

```
}
```

Verification

IN THIS SECTION

- Verifying That the Analyzer Has Been Correctly Created | **1284**
- Verifying That The Port-Mirroring Instance Is Configured Properly | **1285**

To confirm that the configuration is correct, perform these tasks:

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer **employee-monitor** or **employee-web-monitor** has been created on the switch with the appropriate input interfaces, and appropriate output interface.

Action

You can use the **show forwarding-options analyzer** command to verify that the analyzer is configured properly.

`user@switch>` **show forwarding-options analyzer**

```
Analyzer name                    : employee-monitor
Mirror rate                      : 1
Maximum packet length            : 0
State                            : up
Ingress monitored interfaces     : ge-0/0/0.0
Ingress monitored interfaces     : ge-0/0/1.0
Output interface                 : ge-0/0/10.0
```

Meaning

This output shows that the analyzer **employee-monitor** has a ratio of 1 (mirroring every packet, the default setting), the maximum size of the original packet that was mirrored (**0** indicates the entire packet), the state of the configuration (is up indicates that the analyzer is mirroring the traffic entering the ge-0/0/0, and ge-0/0/1 interfaces, and sending the mirrored traffic to the ge-0/0/10 interface). If the state of the

output interface is down or if the output interface is not configured, the value of state will be **down** and the analyzer will not be programmed for mirroring.

Verifying That The Port-Mirroring Instance Is Configured Properly

Purpose

Verify that the port-mirroring instance **employee-web-monitor** has been configured properly on the switch with the appropriate input interfaces.

Action

You can verify that the port-mirroring instance is configured properly by using the **show forwarding-options port-mirroring** command.

```
user@switch> show forwarding-options port-mirroring
```

```
Instance Name: employee-web-monitor
  Instance Id: 3
  Input parameters:
    Rate                 : 1
    Run-length           : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    ethernet-switching  up        ge-0/0/10.0
```

Meaning

This output shows that the **employee-web-monitor** instance has a ratio of 1 (mirroring every packet, the default), the maximum size of the original packet that was mirrored (**0** indicates an entire packet), the state of the configuration is up and port mirroring is programmed, and that mirrored traffic from the firewall filter action is sent out on interface ge-0/0/10.0. If the state of the output interface is down or if the interface is not configured, the value for state will be down and port mirroring will not be programmed for mirroring.

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches

IN THIS SECTION

- Requirements | **1287**
- Overview and Topology | **1287**
- Mirroring All Employee Traffic for Remote Analysis | **1288**
- Mirroring Employee-to-Web Traffic for Remote Analysis | **1292**
- Verification | **1297**

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches" on page 1286. For ELS details see: *Getting Started with Enhanced Layer 2 Software*.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX4300 switches

You can analyze the mirrored traffic by using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN so that you can perform analysis from a remote monitoring station. The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario but includes a filter to mirror only the employee traffic going to the Web.

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

This example describes how to configure remote mirroring:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2X50-D10 or later for EX Series switches
- An EX4300 switch connected to another EX4300 switch

The diagram shows an EX4300 Virtual Chassis connected to an EX4300 destination switch.

Before you configure remote mirroring, be sure that:

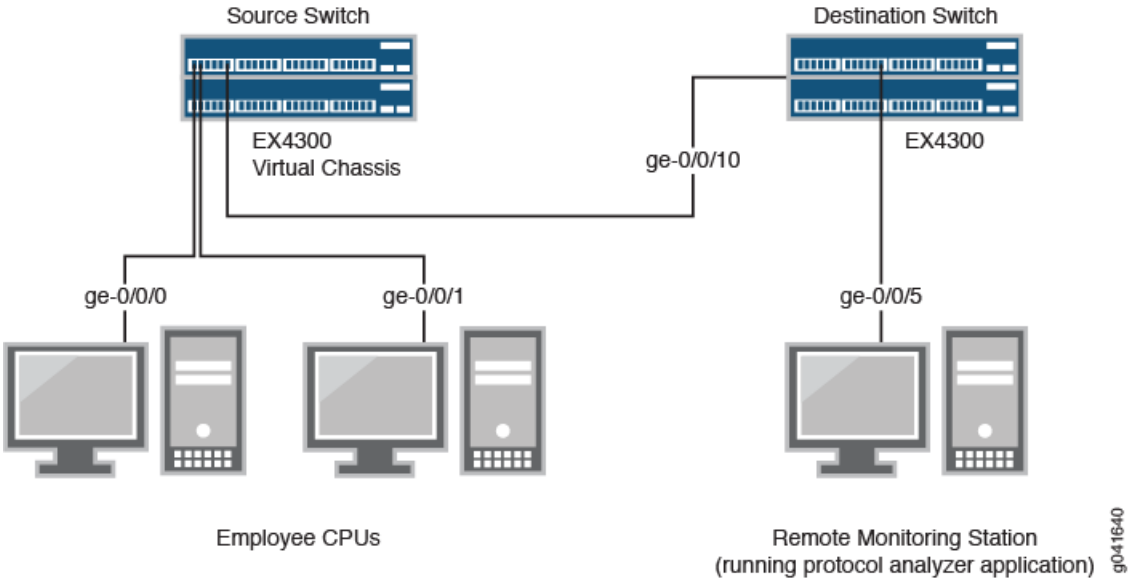
- You have an understanding of mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

Overview and Topology

This topic includes two related examples that describe how to configure mirroring to the **remote-analyzer** VLAN so that analysis can be performed from a remote monitoring station. The first example shows how to configure a switch to mirror all traffic from employee computers. The second example shows the same scenario, but the setup includes a filter to mirror only the employee traffic going to the Web.

Figure 45 on page 1247 shows the network topology for both these example scenarios.

Figure 49: Remote Mirroring Network Topology Example



In this example:

a. Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source switch) that serve as connections for employee computers.

b. Interface ge-0/0/10 is a Layer 2 interface that connects the source switch to the destination switch.

c. Interface ge-0/0/5 is a Layer 2 interface that connects the destination switch to the remote monitoring station.

d. VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic for Remote Analysis

To configure an analyzer for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure an analyzer for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
```

set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer

- Copy and paste the following commands in the destination switch terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

Step-by-Step Procedure

To configure basic remote port mirroring:

1. On the source switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure the interface on the network port connected to the destination switch for trunk mode and associate it with the **remote-analyzer** VLAN:

     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure the **employee-monitor** analyzer:

     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set instance employee-monitor input egress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor output vlan remote-analyzer
     ```

2. On the destination switch:

- Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the interface on the destination switch for trunk mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the interface connected to the destination switch for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/5.0
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
                remote-analyzer;
```

```
        }
      }
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            }
        }
    }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch> show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 999;
```

```
            }
          }
        }
      }
    }
    vlans {
      remote-analyzer {
        vlan-id 999;
        interface {
          ge-0/0/10.0
          }
        }
      }
    }
    forwarding-options {
      analyzer employee-monitor {
        input {
          ingress {
            vlan remote-analyzer;
          }
        }
        output {
          interface {
            ge-0/0/5.0;
          }
        }
      }
    }
```

Mirroring Employee-to-Web Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis of employee- to- Web traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port mirroring to mirror employee traffic to the external Web, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch terminal window:

```
[edit]
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
user@switch# set vlans remote-analyzer vlan-id 999
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
```

```
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-corp from
   destination-address 192.0.2.16/24
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-corp from
   source-address 192.0.2.16/24
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-corp then
   accept
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-web from
   destination-port 80
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-web then
   port-mirror-instance employee-web-monitor
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

- Copy and paste the following commands in the destination switch terminal window:

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
user@switch# set forwarding-options analyzer employee-web-monitor input ingress vlan remote-analyzer
user@switch# set forwarding-options analyzer employee-web-monitor output interface ge-0/0/5.0
```

Step-by-Step Procedure

To configure port mirroring of all traffic from the two ports connected to employee computers to the **remote-analyzer** VLAN for use from a remote monitoring station:

1. On the source switch:
   - Configure the **employee-web-monitor** port mirroring instance:

     ```
     [edit ]
     user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
     user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
     ```

   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure the interface to associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the firewall filter called **watch-employee**:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address 192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
  employee-web-monitor
```

- Apply the firewall filter to the employee interfaces:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

2. On the destination switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure the interface on the destination switch for trunk mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

   - Configure the interface connected to the destination switch for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
```

   - Configure the **employee-monitor** analyzer:

```
[edit forwarding-options port-mirroring]
user@switch# set instance employee-web-monitor input ingress vlan remote-analyzer
user@switch# set instance employee-web-monitor output interface ge-0/0/5.0
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
}
firewall {
    family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
                from {
                    source-address {
                        192.0.2.16/24;
                    }
                    destination-address {
```

```
                192.0.2.16/24;
            }
        }
        then accept;
    }
    term employee-to-web {
        from {
            destination-port 80;
        }
        then port-mirror-instance employee-web-monitor;
    }
  }
 }
}
forwarding-options {
  analyzer employee-web-monitor {
    output {
      vlan {
        999;
      }
    }
  }
vlans {
  remote-analyzer {
    vlan-id 999;
  }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch> show
vlans {
  remote-analyzer {
    vlan-id 999;
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members remote-analyzer;
```

```
            }
          }
        }
      }
      ge-0/0/5 {
        unit 0 {
          family ethernet-switching {
            interface-mode trunk;
          }
        }
      }
    }
    forwarding-options {
      port-mirroring {
        instance employee-web-monitor {
          input {
            ingress {
              vlan remote-analyzer;
            }
          }
          output {
            interface {
              ge-0/0/5.0;
            }
          }
        }
      }
```

Verification

IN THIS SECTION

- Verifying That the Analyzer Has Been Correctly Created | **1297**

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** or **employee-web-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify the analyzer is configured as expected by using the **show forwarding-options analyzer** command. To view previously created analyzers that are disabled, go to the J-Web interface.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the **show analyzer** command on the source switch. The following output is displayed for this configuration example:

`user@switch>` **show forwarding-options analyzer**

```
Analyzer name                    : employee-monitor
Mirror rate                        : 1
Maximum packet length        : 0
State                                 : up
Ingress monitored interfaces     : ge-0/0/0.0
Ingress monitored interfaces     : ge-0/0/1.0
Egress monitored interfaces     : ge-0/0/0.0
Egress monitored interfaces     : ge-0/0/1.0
Output VLAN                        : default-switch/remote-analyzer
```

Meaning

This output shows that the **employee-monitor** instance has a ratio of 1 (mirroring every packet, the default), the maximum size of the original packet that was mirrored (0 indicates the entire packet), the state of the configuration is up (which indicates the proper state and that the analyzer is programmed, and is mirroring the traffic entering ge-0/0/0 and ge-0/0/1 and is sending the mirrored traffic to the VLAN called **remote-analyzer**). If the state of the output interface is down or if the output interface is not configured, the value of state will be down and the analyzer will not be programmed for mirroring.

RELATED DOCUMENTATION

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches

IN THIS SECTION

- Requirements | 1300
- Overview and Topology | 1300
- Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch | 1301
- Verification | 1306

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX4300 switches

You can analyze the mirrored traffic by using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes an example that describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN through a transit switch, so that you can perform analysis from a remote monitoring station.

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

This example describes how to configure remote mirroring through a transit switch:

Requirements

This example uses the following hardware and software components:

- An EX4300 switch connected to another EX4300 switch through a third EX4300 switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure remote mirroring, be sure that:

- You have an understanding of mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

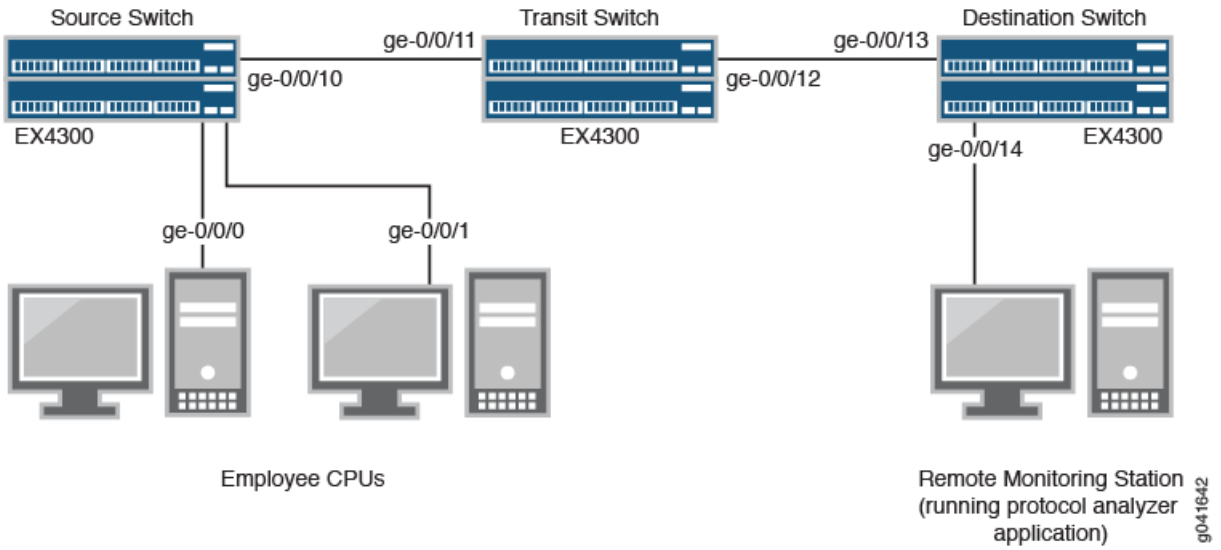
Overview and Topology

This example describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN through a transit switch so that you can perform analysis from a remote monitoring station. The example shows how to configure a switch to mirror all traffic from employee computers to a remote analyzer.

In this configuration, an analyzer session is required on the destination switch to mirror incoming traffic from the analyzer VLAN to the egress interface to which the remote monitoring station is connected. You must disable MAC learning on the transit switch for the **remote-analyzer** VLAN so that MAC learning is disabled for all member interfaces of the **remote-analyzer** VLAN on the transit switch.

Figure 47 on page 1270 shows the network topology for this example.

Figure 50: Remote Mirroring Through a Transit Switch Network–Sample Topology



In this example:

- Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source switch) that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects to the transit switch.
- Interface ge-0/0/11 is a Layer 2 interface on the transit switch.
- Interface ge-0/0/12 is a Layer 2 interface on the transit switch and connects to the destination switch.
- Interface ge-0/0/13 is a Layer 2 interface on the destination switch .
- Interface ge-0/0/14 is a Layer 2 interface on the destination switch and connects to the remote monitoring station.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch

To configure mirroring for remote traffic analysis through a transit switch, for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure mirroring for remote traffic analysis through a transit switch, for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch (monitored switch) terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

- Copy and paste the following commands in the transit switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
set vlans remote-analyzer interface ge-0/0/11
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
```

set vlans remote-analyzer interface ge-0/0/12
set vlans remote-analyzer no-mac-learning

- Copy and paste the following commands in the destination switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
set vlans remote-analyzer interface ge-0/0/13 ingress
set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/14.0
```

Step-by-Step Procedure

To configure remote mirroring through a transit switch:

1. On the source switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure the interfaces on the network port connected to transit switch for trunk mode and associate it with the **remote-analyzer** VLAN:

     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure the **employee-monitor** analyzer:

     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor output vlan remote-analyzer
     ```

2. On the transit switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

     ```
     [edit vlans]
     ```

```
user@switch# set remote-analyzer vlan-id 999
```

- Configure the ge-0/0/11 interface for trunk mode, associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
```

- Configure the **ge-0/0/12** interface for trunk mode, associate it with the **remote-analyzer** VLAN, and set the interface for egress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/12
```

- Configure the **no-mac-learning** option for the **remote-analyzer** VLAN to disable MAC learning on all interfaces that are members of the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set vlans remote-analyzer no-mac-learning
```

3. On the destination switch:
   - Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure the ge-0/0/13 interface for trunk mode, associate it with the **remote-analyzer** VLAN, and set the interface for ingress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

   - Configure the interface connected to the remote monitoring station for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
```

   - Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    member 999;
                }
            }
        }
    }
}
```

Check the results of the configuration on the transit switch:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0 {
            }
            ge-0/0/12.0 {
            }
        }
        no-mac-learning;
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/13.0 {
                ingress;
            }
        }
    }
```

```
}
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/14.0;
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying That the Analyzer Has Been Correctly Created | **1307**

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** has been created on the switch with the appropriate input interfaces and the appropriate output interface.

Action

You can verify whether the analyzer is configured as expected by using the **show analyzer** command. To view previously created analyzers that are disabled, go to the J-Web interface.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the **show analyzer** command on the source switch. The following output is displayed for this example configuration:

```
user@switch> show forwarding-options analyzer
```

```
Analyzer name                    : employee-monitor
  Mirror rate                      : 1
  Maximum packet length            : 0
  State                            : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces      : ge-0/0/0.0
  Egress monitored interfaces      : ge-0/0/1.0
  Output vlan                      : default-switch/remote-analyzer
```

Meaning

This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, the default), is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and sending the mirrored traffic to the analyzer **remote-analyzer**.

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) | **1230**

CHAPTER 37

Configuring Port Mirroring Instances

IN THIS CHAPTER

- Layer 2 Port Mirroring Global Instance | 1308
- Configuring the Global Instance of Layer 2 Port Mirroring | 1309
- Layer 2 Port Mirroring Named Instances | 1312
- Defining a Named Instance of Layer 2 Port Mirroring | 1315
- Disabling Layer 2 Port Mirroring Instances | 1319
- Configuring Inline Port Mirroring | 1320

Layer 2 Port Mirroring Global Instance

On an MX Series router and on an EX Series switch, you can configure a set of port-mirroring properties that implicitly apply to packets received on all ports in the router (or switch) chassis. This set of port-mirroring properties is the *global instance* of Layer 2 port mirroring for the router or switch.

Within the global instance configuration, you can specify a set of mirror destination properties for each packet address family supported by Layer 2 port mirroring.

For a general description of Layer 2 port-mirroring properties, see "Understanding Layer 2 Port Mirroring Properties" on page 1201. For a comparison of the types of Layer 2 port mirroring available on an MX Series router and on an EX Series switch, see *Application of Layer 2 Port Mirroring Types*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Configuring the Global Instance of Layer 2 Port Mirroring

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328

Example: Layer 2 Port Mirroring with Multiple Instances

Example: Layer 2 Port Mirroring to Multiple Destinations | 1412

Configuring the Global Instance of Layer 2 Port Mirroring

On an MX Series router and on an EX Series switch, you can configure a set of Layer 2 port-mirroring properties that implicitly apply to packets received on all ports in the router (or switch) chassis.

To configure the global instance of Layer 2 port mirroring on an MX Series router and on an EX Series switch:

1. Enable configuration of the Layer 2 port mirroring:

```
[edit]
user@host# edit forwarding-options port-mirroring
```

2. Enable configuration of the packet-selection properties:

```
[edit forwarding-options port-mirroring]
user@host# edit input
```

3. Specify global-level packet-selection properties.

   a. Specify the number of packets to select:

   ```
   [edit forwarding-options port-mirroring input]
   user@host# set rate number
   ```

   The valid range is 1 through 65535.

   b. Specify the number of packets to mirror from each selection:

   ```
   [edit forwarding-options port-mirroring input]
   user@host# set run-length number
   ```

   The valid range is 0 through 20. The default value is 0.

   c. Specify the length to which mirrored packets are to be truncated:

   ```
   [edit forwarding-options port-mirroring input]
   user@host# set maximum-packet-length number
   ```

   The valid range is 0 through 9216. The default value is 0, which means the mirrored packets are not truncated.

4. Specify the global-level Layer 2 address-type family from which traffic is to be selected for mirroring:

   ```
   [edit forwarding-options port-mirroring input]
   user@host# up
   [edit forwarding-options port-mirroring]
   user@host# edit family family
   ```

   The value of the *family* option can be **ethernet-switching**, **ccc**or **vpls**.

   NOTE: Under the **[edit forwarding-options port-mirroring]** hierarchy level, the protocol family statement **family ethernet-switching** is an alias for **family vpls**. The command-line interface (CLI) displays Layer 2 port-mirroring configurations as **family vpls**, even for Layer 2 port-mirroring configured as **family ethernet-switching**. Use **family ethernet-switching** when the physical interface is configured with **encapsulation ethernet-bridge**.

5. Enable configuration of global-level mirror destination properties for this address family:

```
[edit forwarding-options port-mirroring family family]
user@host# edit output
```

6. Specify global-level mirror destination properties for this address family.

   a. Specify the physical interface on which to send the mirrored packets:

   ```
   [edit forwarding-options port-mirroring family family output]
   user@host# set interface interface-name
   ```

   You can also specify an integrated routing and bridging (IRB) interface as the output interface.

   b. (Optional) Allow configuration of filters on the destination interface for the named port-mirroring instance:

   ```
   [edit forwarding-options port-mirroring family family output]
   user@host# set no-filter-check
   ```

7. (Optional) Specify that any packets selected for mirroring are to be mirrored only once to any mirroring destination:

```
[edit forwarding-options port-mirroring family family output]
user@host# up 2
[edit forwarding-options port-mirroring]
user@host# set mirror-once
```

TIP: Enable the **mirror-once** option when an MX Series router or an EX Series switch is configured to perform Layer 2 port mirroring at both ingress and egress interfaces, which could result in sending duplicate packets to the same destination (which would complicate the analysis of the mirrored traffic).

8. Verify the minimum configuration of the global instance of Layer 2 port mirroring:

```
[edit forwarding-options ... ]
user@host# top
```

```
[edit]
user@host# show forwarding-options

forwarding-options {
   port-mirroring {
      input { # Global packet-selection properties.
         maximum-packet-length number; # Default is 0.
         rate number;
         run-length number;
      }
      family (ccc | vpls) { # Address- type 'ethernet-switching' displays as 'vpls'.
         output { # Global mirror destination properties.
            interface interface-name;
            no-filter-check; # Optional. Allow filters on interface.
         }
      }
      mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
   }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Global Instance | 1308

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328

Example: Layer 2 Port Mirroring with Multiple Instances

Layer 2 Port Mirroring Named Instances

IN THIS SECTION

- Layer 2 Port Mirroring Named Instances Overview | 1313
- Mirroring at Ports Grouped at the FPC Level | 1313
- Mirroring at Ports Grouped at the PIC Level | 1314
- Mirroring at a Group of Ports Bound to Multiple Named Instances | 1314

This topic describes the following information:

Layer 2 Port Mirroring Named Instances Overview

On an MX Series router and on an EX Series switch, you can define a set of port-mirroring properties that you can explicitly bind to physical ports on the router or switch. This set of port mirroring properties is known as a *named instance* of Layer 2 port mirroring.

You can bind a named instance of Layer 2 port mirroring to physical ports associated with an MX Series router's or an EX Series switch's Packet Forwarding Engine components at different levels of the router (or switch) chassis:

- At the FPC level—You can bind a named instance to the physical ports associated with a specific Dense Port Concentrator (DPC) or to the physical ports associated with a specific Flexible Port Concentrator (FPC).
- At the PIC level—You can bind a named instance of port mirroring to a specific Packet Forwarding Engine (on a specific DPC) or to a specific PIC.

> **NOTE:** MX Series routers support DPCs as well as FPCs and PICs. Unlike FPCs, DPCs do not support PICs. In the Junos OS CLI, however, you use FPC and PIC syntax to configure or display information about DPCs and the Packet Forwarding Engines on the DPCs.

The following points summarize the behavior of Layer 2 port mirroring based on named instances:

- The scope of packet selection is determined by the target of the binding—At the ports (or port) bound to a named instance of Layer 2 port mirroring, the router or switch selects input packets according to the packet-selection properties in the named instance.
- The destination of a selected packet is determined by the packet address family—Of the packets selected, the router or switch mirrors only the packets belonging to an address family for which the named instance of Layer 2 port mirroring specifies a set of mirror destination properties. In a Layer 2 environment, MX Series routers and EX Series switches support port mirroring of VPLS (**family ethernet-switching** or **family vpls**) traffic and Layer 2 VPN traffic with **family ccc**.

For a general description of Layer 2 port-mirroring properties, see "Understanding Layer 2 Port Mirroring Properties" on page 1201. For a comparison of the types of Layer 2 port mirroring available on an MX Series router and on an EX Series switch, see *Application of Layer 2 Port Mirroring Types*.

Mirroring at Ports Grouped at the FPC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to a specific DPC or FPC installed in the router (or switch) chassis. The port mirroring properties in the instance are applied to all Packet Forwarding Engines (and their associated ports) on the specified DPC or

to all PICs (and their associated ports) installed in the specified FPC. Port mirroring properties that are bound to a DPC or FPC override any port-mirroring properties bound at the global level or the MX Series router (or switch) chassis.

Mirroring at Ports Grouped at the PIC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to a specific Packet Forwarding Engine or PIC. The port-mirroring properties in that instance are applied to all ports associated with the specified Packet Forwarding Engine or PIC. Port-mirroring properties that are bound to a Packet Forwarding Engine or PIC override any port-mirroring properties bound at the DPC or FPC that contains them.

> **NOTE:** For MX960 routers, there is a one-to-one mapping of Packet Forwarding Engines to Ethernet ports. Therefore, on MX960 routers only, you can configure port-specific bindings of port-mirroring instances.

Mirroring at a Group of Ports Bound to Multiple Named Instances

On an MX Series router and on an EX Series switch, you can apply up to two named instances of Layer 2 port mirroring to the same group of ports within the router (or switch) chassis. By applying two different port-mirroring instances to the same DPC, FPC, Packet Forwarding Engine, or PIC, you can bind two distinct Layer 2 port mirroring specifications to a single group of ports.

> **NOTE:** You can configure only one global instance of Layer 2 port mirroring on an MX Series router and on an EX Series switch.

> **NOTE:** You can configure more than two port mirroring instances for each FPC by configuring inline port mirroring. For information on inline port mirroring, see "Configuring Inline Port Mirroring" on page 1320.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Defining a Named Instance of Layer 2 Port Mirroring

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level | 1324
Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level | 1326
Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328
Example: Layer 2 Port Mirroring with Multiple Instances

Defining a Named Instance of Layer 2 Port Mirroring

On an MX Series router and on an EX Series switch, you can define a set of Layer 2 port-mirroring properties that you can bind to a particular Packet Forwarding Engine (at the PIC level of the router or switch chassis) or to a group of Packet Forwarding Engines (at the DPC or FPC level of the chassis).

To define a named instance of Layer 2 port mirroring on an MX Series router or on an EX Series switch:

1. Enable configuration of a named instance of Layer 2 port mirroring :

```
[edit]
user@host# edit forwarding-options port-mirroring instance pm-instance-name
```

2. Enable configuration of the packet-sampling properties:

```
[edit forwarding-options port-mirroring instance pm-instance-name]
user@host# edit input
```

3. Specify packet-selection properties:

   a. Specify the number of packets to select:

   ```
   [edit forwarding-options port-mirroring instance pm-instance-name input]
   user@host# set rate number
   ```

   The valid range is **1** through **65535**.

   b. Specify the number of packets to mirror from each selection:

   ```
   [edit forwarding-options port-mirroring instance pm-named-instance input]
   user@host# set run-length number
   ```

   The valid range is **0** through **20**. The default value is **0**.

   NOTE: The **run-length** statement is not supported on MX80 routers.

   c. Specify the length to which mirrored packets are to be truncated:

   ```
   [edit forwarding-options port-mirroring instance pm-instance-name input]
   user@host# set maximum-packet-length number
   ```

   The valid range is **0** through **9216**. The default value is **0**, which means the mirrored packets are not truncated.

   NOTE: The **maximum-packet-length** statement is not supported on MX80 routers.

4. Enable configuration of the mirror destination properties for Layer 2 packets that are part of bridging domain, Layer 2 switching cross-connects, or virtual private LAN service (VPLS):

   a. Specify the Layer 2 address family type of traffic to be mirrored:

   ```
   [edit forwarding-options port-mirroring instance pm-instance-name input]
   user@host# up
   [edit forwarding-options port-mirroring instance pm-instance-name]
   user@host# edit family family
   ```

   The value of the *family* option can be **ethernet-switching**, **ccc**, or **vpls**.

> **NOTE:** Under the **[edit forwarding-options port-mirroring]** hierarchy level, the protocol family statement **family ethernet-switching** is an alias for **family vpls**. The command-line interface (CLI) displays Layer 2 port-mirroring configurations as **family vpls**, even for Layer 2 port-mirroring configured as **family ethernet-switching**. Use **family ethernet-switching** when the physical interface is configured with **encapsulation ethernet-bridge**.

b. Enable configuration of the mirror destination properties:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family]
user@host# edit output
```

5. Specify mirror destination properties.

   a. Specify the physical interface on which to send the mirrored packets:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# set interface interface-name
```

   b. (Optional) Allow configuration of filters on the destination interface for the global port-mirroring instance:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# set no-filter-check
```

> **NOTE:** You cannot configure port mirroring instances on MX80 routers. You can only configure port mirroring at the global level on MX80 routers.

6. (Optional) Specify that any packets selected for mirroring are to be mirrored only once to any mirroring destination:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# up 3
[edit forwarding-options port-mirroring]
user@host# set mirror-once
```

> **TIP:** Enable the global **mirror-once** option when an MX Series router or an EX Series switch is configured to perform Layer 2 port mirroring at both ingress and egress interfaces, which could result in sending duplicate packets to the same destination (which in turn would complicate the analysis of the mirrored traffic).

7. To configure a mirroring destination for a different packet family type, repeat steps 4 through 6.

8. Verify the minimum configuration of the named instances of Layer 2 port mirroring:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show forwarding-options

forwarding-options {
    port-mirroring {
        ... optional-global-port-mirroring-configuration ...
        instance {
            pm-instance-name ( # A named instance of port mirroring
                input { # Packet-selection properties
                    maximum-packet-length number; # Default is 0.
                    rate number;
                    run-length number;
                }
                family (ccc | vpls) { # Address- type 'ethernet-switching' displays as 'vpls'.
                    output { # Mirror destination properties
                        interface interface-name;
                        no-filter-check; # Optional. Allow filters on interface.
                    }
                }
            }
        }
        mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Named Instances

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level | **1324**

Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level | **1326**

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | **1328**

Example: Layer 2 Port Mirroring with Multiple Instances

Disabling Layer 2 Port Mirroring Instances

You can disable the global instance of Layer 2 port mirroring, a particular named instance, or all instances of port mirroring:

- To disable the global instance of Layer 2 port mirroring, include the **disable** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit]
forwarding-options {
    port-mirroring {
        disable; Disables the global instance of Layer 2 port mirroring.
        ...global-instance-of-layer-2-port-mirroring-configuration...
    }
}
```

- To disable the definition of a particular named instance of Layer 2 port mirroring, include the **disable** statement at the **[edit forwarding-options port-mirroring instance *instance-name*]** hierarchy level:

```
[edit]
forwarding-options {
    port-mirroring {
        ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
        instance {
            port-mirroring-instance-name {
                disable; Disables this named instance of Layer 2 port mirroring.
                ...definition-of-a-named-instance-of-layer-2-port-mirroring...
            }
        }
    }
}
```

- To disable the global instance and all named instances of Layer 2 port mirroring, include the **disable-all-instances** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit]
forwarding-options {
   port-mirroring {
      disable-all-instances; Disables all instances of Layer 2 port mirroring.
      ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
      instance {
         port-mirroring-instance-name {
            ...definition-of-a-named-instance-of-layer-2-port-mirroring...
         }
      }
   }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Global Instance | 1308

Layer 2 Port Mirroring Named Instances

Displaying Layer 2 Port-Mirroring Instance Settings and Status | 1457

Configuring Inline Port Mirroring

Inline port mirroring provides you with the ability to specify instances that are not bound to the flexible PIC concentrator (FPC) in the firewall filter **then port-mirror-instance** action. This way, you are not limited to only two port-mirror instances per FPC. Inline port mirroring decouples the port-mirror destination from the input parameters like **rate**. While the input parameters are programmed in the switch interface board, the next-hop destination of the mirrored packet is available in the packet itself. Inline port mirroring is supported only on Trio-based modular port concentrators (MPCs).

Using inline port mirroring, a port-mirror instance will have an option to inherit input parameters from another instance that specifies it, as shown in the following CLI configuration example:

```
instance pm2 {
   + input-parameters-instance pm1;
   family inet {
```

```
        output {
            interface ge-1/2/3.0 {
                next-hop 192.0.2.10;
            }
        }
    }
}
```

Multiple levels of inheritance are not allowed. One instance can be referred by multiple instances. An instance can refer to another instance that is defined before it. Forward references are not allowed and an instance cannot refer to itself, doing so will cause an error during configuration parsing.

The user can specify an instance that is not bound to the FPC in the firewall filter. The specified filter should inherit one of the two instances that have been bound to the FPC. If it does not, the packet is not marked for port-mirroring. If it does, then the packet will be sampled using the input parameters specified by the referred instance but the copy will be sent to the its own destination.

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | **1200**
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | **1370**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1373**
- Example: Layer 2 Port Mirroring at a Logical Interface | **1385**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**

CHAPTER 38

Configuring Port Mirroring for Physical Interfaces

IN THIS CHAPTER

- Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface | 1322
- Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level | 1324
- Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level | 1326
- Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328
- Configuring Layer 2 Port Mirroring Over GRE Interface | 1330
- Example: Configuring Layer 2 Port Mirroring Over a GRE Interface | 1331

Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface

You can bind different sets of Layer 2 port mirroring properties (the global instance and one or more named instances) at various levels of an MX Series router or of an EX Series switch chassis (at the chassis level, at the FPC level, or at the PIC level). Therefore, it is possible for a single group of physical interfaces to be bound to multiple Layer 2 port mirroring definitions.

If a group of ports (or, in the case of a PIC-level binding in an MX960 router, a single port) is bound to multiple Layer 2 port mirroring definitions, the router (or switch) applies the Layer 2 port-mirroring properties to those ports as follows:

1. Chassis-level port-mirroring properties implicitly apply to all ports in the chassis. If an MX Series router or an EX Series switch is configured with the global port-mirroring instance, those port mirroring properties apply to all ports. See *Configuring the Global Instance of Layer 2 Port Mirroring*.
2. FPC-level port-mirroring properties override chassis-level properties. If a DPC or FPC is bound to a named instance of port mirroring, those port mirroring properties apply to all ports associated with that DPC or FPC, overriding any port mirroring properties bound at the chassis level. See "Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level" on page 1324.
3. PIC-level port-mirroring properties override FPC-level properties. If a Packet Forwarding Engine or PIC is bound to a named instance of port-mirroring, those port mirroring properties apply to all ports associated with the Packet Forwarding Engine or PIC, overriding any port-mirroring properties bound

to those ports at the FPC level. See “Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level” on page 1326.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Restrictions on Layer 2 Port Mirroring

Application of Layer 2 Port Mirroring Types

Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces | **1356**

Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces | **1358**

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to a specific DPC or to a specific FPC in the router (or switch) chassis. This is known as binding a named instance of Layer 2 port mirroring *at the FPC level* of the router (or switch) chassis. The port mirroring properties specified in the named instance are applied to all physical ports associated with all Packet Forwarding Engines on the specified DPC or FPC.

> **NOTE:** You can also bind a named instance of Layer 2 port mirroring to a specific Packet Forwarding Engine on a DPC or FPC in the router (or switch) chassis.
>
> For any packet-type family supported by Layer 2 port mirroring
>
> - Port-mirroring properties bound to a specific DPC or FPC override any port-mirroring properties configured at the global level.
> - Port-mirroring properties bound to a specific Packet Forwarding Engine override any port-mirroring properties configured at the DPC or FPC level.

You can apply up to two named instances of Layer 2 port mirroring to the same group of ports within the router (or switch) chassis. By applying two different port-mirroring instances to the same DPC or FPC, you can bind two distinct Layer 2 port-mirroring specifications to a single group of ports.

Before you begin, complete the following tasks:

- Define a named instance of Layer 2 port mirroring. See *Defining a Named Instance of Layer 2 Port Mirroring*.
- Display information about the number and types of DPCs or FPCs in the MX Series router and in the EX Series switch, the number of Packet Forwarding Engines on each, and the number and types of ports per Packet Forwarding Engine.

To bind a named instance of Layer 2 port mirroring to a DPC or FPC and its Packet Forwarding Engines:

1. Enable configuration of the router (or switch) chassis properties:

   ```
   [edit]
   user@host# edit chassis
   ```

2. Enable configuration of a DPC (and its corresponding Packet Forwarding Engines) or an FPC (and its installed PICs):

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

3. Bind a named instance of Layer 2 port mirroring (*pm-instance-name*) to the DPC or FPC:

```
[edit chassis fpc slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Optional) To bind a second named instance of Layer 2 port mirroring to the same DPC or FPC, repeat the previous step (step 3) and specify a different named instance of Layer 2 port mirroring.

5. Verify the minimum configuration of the binding:

```
[edit chassis fpc slot-number port-mirror-instance pm-instance-name]
user@host# top
[edit]
user@host# show chassis

chassis {
    fpc slot-number { # Bind two port mirroring named instances at the FPC level.
        port-mirror-instance pm-instance-name-1;
        port-mirror-instance pm-instance-name-2;
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Named Instances

Defining a Named Instance of Layer 2 Port Mirroring

Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level | 1326

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328

Example: Layer 2 Port Mirroring with Multiple Instances

Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to the ports associated with a specific Packet Forwarding Engine (on a DPC) or to the ports associated with a specific PIC (installed in an FPC). This is known as binding a named instance of Layer 2 port mirroring *at the PIC level* of the router (or switch) chassis. The port-mirroring properties specified in the named instance are applied to all physical ports associated with the specified Packet Forwarding Engine.

> **NOTE:** You can also bind a named instance of Layer 2 port mirroring to a specific DPC or FPC in the router (or switch) chassis.
>
> For any packet-type family supported by Layer 2 port mirroring:
>
> - Port-mirroring properties bound to a specific Packet Forwarding Engine override any port-mirroring properties configured at the DPC or FPC level.
> - Port-mirroring properties bound to a specific DPC or FPC override any port-mirroring properties configured at the global level.

You can apply up to two named instances of Layer 2 port-mirroring to the same group of ports within the router (or switch) chassis. By applying two different port-mirroring instances to the same Packet Forwarding Engine or PIC, you can bind two distinct Layer 2 port mirroring specifications to a single group of ports.

For MX960 routers, there is a one-to-one mapping of Packet Forwarding Engines to Ethernet ports. Therefore, on MX960 routers only, you can bind a named instance of Layer 2 port mirroring to a *specific port* by binding the instance to the Packet Forwarding Engine associated with the port.

Before you begin, complete the following tasks:

- Define a named instance of Layer 2 port mirroring. See *Defining a Named Instance of Layer 2 Port Mirroring*.
- Display information about the number and types of DPCs in the MX Series router or in the EX Series switch, the number of Packet Forwarding Engines on each DPC, and the number and types of ports per Packet Forwarding Engine.

To bind a named instance of Layer 2 port mirroring to a Packet Forwarding Engine:

1. Enable configuration of the router (or switch) chassis properties:

```
[edit]
user@host# edit chassis
```

2. Enable configuration of a Packet Forwarding Engine or PIC:

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

3. Bind a named instance of Layer 2 port mirroring (*pm-instance-name*) to the Packet Forwarding Engine or PIC:

```
[edit chassis fpc slot-number pic slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Optional) To bind a second named instance of Layer 2 port mirroring to the same Packet Forwarding Engine or PIC, repeat the previous step (step 3) and specify a different named instance of Layer 2 port mirroring.

5. Verify the minimum configuration of the binding:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show chassis
chassis {
    fpc slot-number {
        ... optional-binding-of-a-port-mirroring-instance-at-the-dpc-level ...
        pic slot-number { # Bind two port-mirroring named instances at the PIC level.
            port-mirror-instance pm-instance-name-1;
            port-mirror-instance pm-instance-name-2;
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Named Instances

Defining a Named Instance of Layer 2 Port Mirroring

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level | 1324

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328

Example: Layer 2 Port Mirroring with Multiple Instances

Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis

IN THIS SECTION

- Layer 2 Port Mirroring at the FPC Level | 1328
- Layer 2 Port Mirroring at the PIC Level | 1329
- Layer 2 Port Mirroring at the FPC and PIC Levels | 1329

On an MX Series router or on an EX Series switch, you can apply named instances of Layer 2 port mirroring at the FPC or DPC level of the chassis or at the PIC level of the chassis. However, you can configure (and implicitly apply) only one global instance of Layer 2 port mirroring to the entire chassis.

Layer 2 Port Mirroring at the FPC Level

In this example configuration of an MX Series router or of an EX Series switch chassis, a named instance of Layer 2 port mirroring (**pm1**) is bound to physical ports grouped at the FPC level:

```
[edit]
chassis {
   fpc 2 {
      port-mirror-instance pm1;
   }
}
```

This is not a complete configuration. The physical interfaces associated with the FPC or DPC in slot 2 must be configured at the **[edit interfaces]** hierarchy level. The Layer 2 port mirroring named instance **pm1** must be configured at the **[edit forwarding-options port-mirroring instance]** hierarchy level.

Layer 2 Port Mirroring at the PIC Level

In this example configuration of an MX Series router or of an EX Series switch chassis, a named instance of Layer 2 port mirroring (**pm2**) is bound to the physical ports grouped at the PIC level:

```
[edit]
chassis {
    fpc 2 {
        pic 0 {
            port-mirror-instance pm2;
        }
    }
}
```

This is not a complete configuration. The physical interfaces associated with the FPC or DPC in slot 2 must be configured at the **[edit interfaces]** hierarchy level. The Layer 2 port mirroring named instance **pm2** must be configured at the **[edit forwarding-options port-mirroring instance]** hierarchy level.

Layer 2 Port Mirroring at the FPC and PIC Levels

In this example configuration of an MX Series router chassis or an EX Series switch, one named instance of Layer 2 port mirroring (**pm1**) is applied at the FPC level of the router (or switch) chassis. A second named instance (**pm2**) is applied at the PIC level:

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance pm1;
        pic 0 {
            port-mirror-instance pm2;
        }
    }
}
```

This is not a complete configuration. Physical interfaces associated with the FPC or DPC in slot 2, including physical interfaces associated with **pic 0**, must be configured at the **[edit interfaces]** hierarchy level. The Layer 2 port mirroring named instances **pm1** and **pm2** must be configured at the **[edit forwarding-options port-mirroring instance]** hierarchy level.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Global Instance | 1308

Layer 2 Port Mirroring Named Instances

Configuring the Global Instance of Layer 2 Port Mirroring

Defining a Named Instance of Layer 2 Port Mirroring

Configuring Layer 2 Port Mirroring Over GRE Interface

Port mirroring is the ability of a router to send a copy of a packet to an external host address or a packet analyzer for analysis. One application for port mirroring sends a duplicate packet to a virtual tunnel. A next-hop group can then be configured to forward copies of this duplicate packet to several interfaces. Junos OS supports Layer 2 port mirroring to a remote collector over a GRE interface.

To configure layer 2 port-mirroring over a GRE interface, do the following:

1. Configure the GRE interface with the source and destination address.

   [edit interfaces *inteface-name* unit *unit-number* tunnel]
   set source *ip-address*
   set destination *ip-address*

2. Configure family bridge parameters on the GRE interface.

   [edit interfaces *interface-name* unit *unit-number* family bridge]
   set interface-mode trunk
   set vlan-id *valn-id*

3. Configure the rate at which the input packets are mirrored.

   [edit forwarding-options port-mirroring]
   set f input rate *rate*

4. Configure the output interface for family VPLS for the GRE interface.

   [edit forwarding-options family vpls]
   set output interface *gre-interface-name*

5. Configure the firewall filter term for family bridge to count packets arriving at the interface.

```
[edit firewall family bridge]
set filter f1 term term then count count
```

6. Configure firewall filter term for family bridge to mirror the packets.

```
[edit firewall family bridge]
set filter filter-name term term then port-mirror
```

RELATED DOCUMENTATION

Example: Configuring Layer 2 Port Mirroring Over a GRE Interface | 1331

Tunnel Services Overview

Example: Configuring Layer 2 Port Mirroring Over a GRE Interface

IN THIS SECTION

- Requirements | 1331
- Overview | 1332
- Configuration | 1332
- Verification | 1337

This example shows how to configure Layer 2 port mirroring over a GRE interface for analysis.

Requirements

This example uses the following hardware and software components:

- One MX Series router
- Junos OS Release 16.1 or later running on all devices

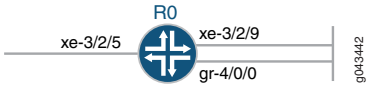
Overview

Port mirroring is the ability of a router to send a copy of a packet to an external host address or a packet analyzer for analysis. One application for port mirroring sends a duplicate packet to a virtual tunnel. A next-hop group can then be configured to forward copies of this duplicate packet to several interfaces. Starting with Junos OS Release 16.1, Layer 2 port mirroring to a remote collector over a GRE interface is supported.

Topology

Figure 51 on page 1332 shows port mirroring configured over a GRE interface. The interface gr-4/0/0 is configured as family bridge. Firewall family bridge filter f1 is configured as port-mirror. Mirror destination is configured as gr-4/0/0. Firewall family bridge filter f1 is applied at the ingress and egress of the xe-3/2/5.0 interface, which mirrors packets to mirror destination gr-4/0/0.

Figure 51: Example Layer 2 Port Mirroring over GRE Interface



Configuration

CLI Quick Configuration

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

R0

```
set chassis fpc4 pic0 tunnel-services bandwidth 10g
set chassis network-services enhanced-ip
set interfaces xe-3/2/5 flexible-vlan-tagging
set interfaces xe-3/2/5 encapsulation flexible-ethernet-services
set interfaces xe-3/2/5 unit 0 encapsulation vlan-bridge
set interfaces xe-3/2/5 unit 0 vlan-id 100
set interfaces xe-3/2/5 unit 0 family bridge filter input f1
set interfaces xe-3/2/5 unit 0 family bridge filter output f1
set interfaces xe-3/2/9 flexible-vlan-tagging
set interfaces xe-3/2/9 encapsulation flexible-ethernet-services
set interfaces xe-3/2/9 unit 0 encapsulation vlan-bridge
set interfaces xe-3/2/9 unit 0 vlan-id 100
```

```
set interfaces gr-4/0/0 unit 0 tunnel source 10.1.1.1
set interfaces gr-4/0/0 unit 0 tunnel destination 10.1.1.2
set interfaces gr-4/0/0 unit 0 family bridge interface-mode trunk
set interfaces gr-4/0/0 unit 0 family bridge vlan-id 100
set forwarding-options port-mirroring input rate 1
set forwarding-options family vpls output interface gr-4/0/0.0
set firewall family bridge filter f1 term t then count c
set firewall family bridge filter f1 term t then port-mirror
set bridge-domains b vlan-id 100
set bridge-domains b interface xe-3/2/5.0
set bridge-domains b interface xe-3/2/9.0
```

Configuring R0

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see “Using the CLI Editor in Configuration Mode” in the *Junos OS CLI User Guide* .

To configure Device R0:

1. Configure the flexible PIC concentrator parameters of the chassis.

```
[edit chassis]
user@R0# set fpc4 pic0 tunnel-services bandwidth 10g
user@R0# set network-services enhanced-ip
```

2. Configure the enhanced-ip network services of the chassis.

```
[edit chassis]
user@R0# set network-services enhanced-ip
```

3. Configure the interfaces.

```
[edit interfaces]

user@R0# set xe-3/2/5 flexible-vlan-tagging
user@R0# set xe-3/2/5 encapsulation flexible-ethernet-services
user@R0# set xe-3/2/5 unit 0 encapsulation vlan-bridge
user@R0# set xe-3/2/5 unit 0 vlan-id 100
```

```
user@R0# set xe-3/2/5 unit 0 family bridge filter input f1
user@R0# set xe-3/2/5 unit 0 family bridge filter output f1

user@R0# set xe-3/2/9 flexible-vlan-tagging
user@R0# set xe-3/2/9 encapsulation flexible-ethernet-services
user@R0# set xe-3/2/9 unit 0 encapsulation vlan-bridge
user@R0# set xe-3/2/9 unit 0 vlan-id 100

user@R0# set gr-4/0/0 unit 0 tunnel source 10.1.1.1
user@R0# set gr-4/0/0 unit 0 tunnel destination 10.1.1.2
user@R0# set gr-4/0/0 unit 0 family bridge interface-mode trunk
user@R0# set gr-4/0/0 unit 0 family bridge vlan-id 100
```

4. Configure the rate of input packets to be sampled.

```
[edit forwarding-options]
user@R0# set port-mirroring input rate 1
```

5. Configure the output interface for the VPLS address family of packets to mirror.

```
[edit forwarding-options]
user@R0# set family vpls output interface gr-4/0/0.0
```

6. Configure the protocol family BRIDGE for the firewall filter.

```
[edit firewall]
user@R0# set family bridge filter f1 term t then count c
user@R0# set family bridge filter f1 term t then port-mirror
```

7. Configure the VLAN ID for the bridge domain.

```
[edit bridge-domains]
user@R0# set b vlan-id 100
user@R0# set b interface xe-3/2/5.0
user@R0# set b interface xe-3/2/9.0
```

8. Configure the interface for the bridge domain.

```
[edit bridge-domains]
```

```
user@R0# set b interface xe-3/2/5.0
user@R0# set b interface xe-3/2/9.0
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, **show forwarding-options**, **show firewall**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R0# show chassis
fpc 4 {
    pic 0 {
        tunnel-services {
            bandwidth 10g;
        }
    }
}
network-services enhanced-ip;
```

```
user@R0# show interfaces
}
xe-3/2/5 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
        family bridge {
            filter {
                input f1;
                output f1;
            }
        }
    }
}
xe-3/2/9 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
```

```
        encapsulation vlan-bridge;
        vlan-id 100;
    }
}
gr-4/0/0 {
    unit 0 {
        tunnel {
            source 10.1.1.1;
            destination 10.1.1.2;
        }
        family bridge {
            interface-mode trunk;
            vlan-id 100;
        }
    }
}
```

```
user@R0# show forwarding-options
port-mirroring {
    input {
        rate 1;
    }
    family vpls {
        output {
            interface gr-4/0/0.0;
        }
    }
}
```

```
user@R0# show firewall
family bridge {
    filter f1 {
        term t {
            then {
                count c;
                port-mirror;
            }
        }
    }
}
```

```
user@R0# show bridge-domains
```

```
b {
    vlan-id 100;
    interface xe-3/2/5.0;
    interface xe-3/2/9.0;
}
```

Verification

IN THIS SECTION

- Verifying Port Mirroring of Traffic | 1337

Confirm that the configuration is working properly.

Verifying Port Mirroring of Traffic

Purpose

Display port mirroring of traffic information.

Action

On Device R0, from operational mode, run the **show forwarding-options port-mirroring** command to display the port mirroring of traffic information.

`user@R0>` **show forwarding-options port-mirroring**

```
Instance Name: & globalinstance
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    vpls                up        gr-4/0/0.0

Instance Name: pm_instance
  Instance Id: 2
  Input parameters:
    Rate                  : 10
```

```
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    vpls                up        gr-4/0/0.0
```

Meaning

The output shows the port mirroring of traffic information.

RELATED DOCUMENTATION

Tunnel Services Overview

Configuring Layer 2 Port Mirroring Over GRE Interface | 1330

CHAPTER 39

Configuring Port Mirroring for Logical Interfaces

IN THIS CHAPTER

- Layer 2 Port Mirroring Firewall Filters | **1340**
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1346**
- Configuring Protocol-Independent Firewall Filter for Port Mirroring | **1349**
- Example: Mirroring Employee Web Traffic with a Firewall Filter | **1351**
- Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces | **1356**
- Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces | **1358**
- Layer 2 Port Mirroring of PE Router or PE Switch Logical Interfaces | **1359**
- Layer 2 Port Mirroring of PE Router or PE Switch Aggregated Ethernet Interfaces | **1361**
- Applying Layer 2 Port Mirroring to a Logical Interface | **1363**
- Applying Layer 2 Port Mirroring to a Logical Interface | **1367**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | **1370**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1373**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1376**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VLAN | **1379**
- Example: Layer 2 Port Mirroring at a Logical Interface | **1382**
- Example: Layer 2 Port Mirroring at a Logical Interface | **1385**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1388**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1397**

Layer 2 Port Mirroring Firewall Filters

IN THIS SECTION

- Layer 2 Port Mirroring Firewall Filters Overview | 1340
- Mirroring of Packets Received or Sent on a Logical Interface | 1341
- Mirroring of Packets Forwarded or Flooded to a VLAN | 1341
- Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance | 1342

This topic describes the following information:

Layer 2 Port Mirroring Firewall Filters Overview

On an MX Series router and on an EX Series switch, you can configure a firewall filter *term* to specify that Layer 2 port mirroring is to be applied to all packets at the interface to which the firewall filter is applied.

You can apply a Layer 2 port-mirroring firewall filter to the input or output logical interfaces (including aggregated Ethernet logical interfaces), to traffic forwarded or flooded to a VLAN, or traffic forwarded or flooded to a VPLS routing instance.

MX Series routers and EX Series switches support Layer 2 port mirroring of VPLS (**family ethernet-switching** or **family vpls**) traffic and Layer 2 VPN traffic with **family ccc** in a Layer 2 environment

Within a firewall filter **term**, you can specify the Layer 2 port-mirroring properties under the **then** statement in either of the following ways:

- Implicitly reference the Layer 2 port mirroring properties in effect on the port.
- Explicitly reference a particular named instance of Layer 2 port mirroring.

> **NOTE:** When configuring a Layer 2 port-mirroring firewall filter, do not include the optional **from** statement that specifies match conditions based on the route source address. Omit this statement so that all packets are considered to match and all *actions* and *action-modifiers* specified in the **then** statement are taken.
>
> If you want to mirror all incoming packets, then you must not use the from statement; /* comment: one configure filter terms with from if they are interested in mirroring only a subset of packets.

For a general description of Layer 2 port-mirroring properties, see "Understanding Layer 2 Port Mirroring Properties" on page 1201. For a comparison of the types of Layer 2 port mirroring available on an MX Series router and on an EX Series switch, see *Application of Layer 2 Port Mirroring Types*.

> **NOTE:** If you associate integrated routing and bridging (IRB) with the VLAN (or VPLS routing instance), and also configure within the VLAN (or VPLS routing instance) a forwarding table filter with the **port-mirror** or **port-mirror-instance** action, then the IRB packet is mirrored as a Layer 2 packet. You can disable this behavior by configuring the *no-irb-layer-2-copy* statement in the VLAN (or VPLS routing instance).

For a detailed description of how to configure a Layer 2 port-mirroring firewall filter, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

For detailed information about how you can use Layer 2 port-mirroring firewall filters with MX Routers and EX Series switches configured as provider edge (PE) routers or PE switches, see "Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces" on page 1356. For detailed information about configuring firewall filters in general (including in a Layer 3 environment), see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

Mirroring of Packets Received or Sent on a Logical Interface

To mirror Layer 2 traffic received or sent on a logical interface, apply a port-mirroring firewall filter to the input or output of the interface.

A port-mirroring firewall filter can also be applied to an aggregated-Ethernet logical interface. For details, see "Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces" on page 1358.

> **NOTE:** If port-mirroring firewall filters are applied at both the input and output of a logical interface, two copies of each packet are mirrored. To prevent the router or switch from forwarding duplicate packets to the same destination, you can enable the "mirror-once" option for Layer 2 port mirroring in the global instance for the Layer 2 packet address family.

Mirroring of Packets Forwarded or Flooded to a VLAN

To mirror Layer 2 traffic forwarded to or flooded to a VLAN, apply a port-mirroring firewall filter to the input to the forwarding table or flood table. Any packet received for the VLAN forwarding or flood table and that matches the filter conditions is mirrored.

For more information about VLANs, see *Understanding Layer 2 Bridge Domains* . For information about flooding behavior in a VLAN, see *Understanding Layer 2 Learning and Forwarding for Bridge Domains* .

> **NOTE:** When you configure port mirroring on any interface under one VLAN, the mirrored packet can move to an external analyzer located on different VLANs.

Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance

To mirror Layer 2 traffic forwarded to or flooded to a VPLS routing instance, apply a port-mirroring firewall filter to the input to the forwarding table or flood table. Any packet received for the VPLS routing instance forwarding or flood table and that matches the filter condition is mirrored.

For more information about VPLS routing instances, see *Configuring a VPLS Routing Instance* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | **1200**
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**
- Example: Layer 2 Port Mirroring at a Logical Interface | **1385**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**
- Example: Layer 2 Port Mirroring to Multiple Destinations | **1412**

Defining a Layer 2 Port-Mirroring Firewall Filter

For virtual private LAN service (VPLS) traffic (**family bridge** or **family vpls**) and for Layer 2 VPNs with family **ccc**on MX Series routers and on EX Series switches only, you can define a firewall filter that specifies Layer 2 port mirroring as the action to be performed if a packet matches the conditions configured in the firewall filter term

You can use a Layer 2 port-mirroring firewall filter in the following ways:

- To mirror packets received or sent on a logical interface.
- To mirror packets forwarded or flooded to a bridge domain.
- To mirror packets forwarded or flooded to a VPLS routing instance.
- To mirror tunnel interface input packets only to multiple destinations.

For a summary of the three types of Layer 2 port-mirroring you can configure on an MX Series router, see *Application of Layer 2 Port Mirroring Types*.

To define a firewall filter with a Layer 2 port-mirroring action:

1. Enable configuration of firewall filters for Layer 2 packets that are part of a bridge domain, a Layer 2 switching cross-connect, or a virtual private LAN service (VPLS):

   ```
   [edit]
   user@host# edit firewall family family
   ```

   The value of the **family** option can be **bridge**,**ccc**, or **vpls**.

2. Enable configuration of a firewall filter **pm-filter-name**:

   ```
   [edit firewall family family]
   user@host# edit filter pm-filter-name
   ```

3. Enable configuration of a firewall filter term **pm-filter-term-name**:

   ```
   [edit firewall family family filter pm-filter-name]
   user@host# edit term pm-filter-term-name
   ```

4. (Optional) Specify the firewall filter match conditions based on the route source address *only if* you want to mirror a subset of the sampled packets.

- For detailed information about Layer 2 bridging firewall filter match conditions (which are supported on MX Series routers only), see *Firewall Filter Match Conditions for Layer 2 Bridging Traffic*.
- For detailed information about VPLS firewall filter match conditions, see *Firewall Filter Match Conditions for VPLS Traffic*.
- For detailed information about Layer 2 circuit cross-connect (CCC) firewall filter match conditions, see *Firewall Filter Match Conditions for Layer 2 CCC Traffic*.

> **NOTE:** If you want all sampled packets to be considered to match (and be subjected to the actions specified in the **then** statement), then omit the **from** statement altogether.

5. Enable configuration of the **action** and **action-modifier** to apply to matching packets:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name]
user@host# edit then
```

6. Specify the actions to be taken on matching packets:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set action
```

   The recommended value for the **action** is **accept**. If you do not specify an action, or if you omit the **then** statement entirely, all packets that match the conditions in the **from** statement are accepted.

7. Specify Layer 2 port mirroring or a next-hop group as the **action-modifier**:

   - To reference the Layer 2 port mirroring properties currently in effect for the Packet Forwarding Engine or PIC associated with the underlying physical interface, use the **port-mirror** statement:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set port-mirror
```

   - To reference the Layer 2 port mirroring properties configured in a specific named instance, use the port-mirror-instance *pm-instance-name* action modifier:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set port-mirror-instance pm-instance-name
```

     If the underlying physical interface is not bound to a named instance of Layer 2 port mirroring but instead is implicitly bound to the global instance of Layer 2 port mirroring, then traffic at the logical

interface is mirrored according to the properties specified in the named instance referenced by the **port-mirror-instance** action modifier.

- To reference a next-hop group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer), use the **next-hop-group** *pm-next-hop-group-name* action modifier:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set next-hop-group pm-next-hop-group-name
```

For configuration information about next-hop groups, see "Defining a Next-Hop Group for Layer 2 Port Mirroring" on page 1402. If you specify a next-hop group for Layer 2 port mirroring, the firewall filter term applies to the tunnel interface input only.

8. Verify the minimum configuration of the Layer 2 port-mirroring firewall filter:

```
[edit firewall ... ]
user@host# top
[edit]
user@host# show firewall

family (bridge | ccc | mpls | vpls) { # Type of packets to mirror
   filter pm-filter-name { # Firewall filter name
      term pm-filter-term-name {
         from { # Do not specify match conditions based on route source address
         }
         then {
            action; # Recommended action is 'accept'
            action-modifier; # Three options for Layer 2 port mirroring
         }
      }
   }
}
```

In the firewall filter term **then** statement, the *action-modifier* can be **port-mirror**, **port-mirror-instance** , or **next-hop-group** *pm-next-hop-group-name*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | **1401**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | 1391
Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394
Example: Layer 2 Port Mirroring to Multiple Destinations | 1412

Defining a Layer 2 Port-Mirroring Firewall Filter

For virtual private LAN service (VPLS) traffic (**family ethernet-switching** or **family vpls**) and for Layer 2 VPNs with family **ccc**on MX Series routers and on EX Series switches only, you can define a firewall filter that specifies Layer 2 port mirroring as the action to be performed if a packet matches the conditions configured in the firewall filter term.

You can use a Layer 2 port-mirroring firewall filter in the following ways:

- To mirror packets received or sent on a logical interface.
- To mirror packets forwarded or flooded to a VLAN.
- To mirror packets forwarded or flooded to a VPLS routing instance.
- To mirror tunnel interface input packets only to multiple destinations.

For a summary of the three types of Layer 2 port-mirroring you can configure on an MX Series router and on an EX Series switch, see *Application of Layer 2 Port Mirroring Types*.

To define a firewall filter with a Layer 2 port-mirroring action:

1. Enable configuration of firewall filters for Layer 2 packets that are part of a VLAN, a Layer 2 switching cross-connect, or a virtual private LAN service (VPLS):

   ```
   [edit]
   user@host# edit firewall family family
   ```

   The value of the **family** option can be **ethernet-switching** , **ccc**, or **vpls**.

2. Enable configuration of a firewall filter **pm-filter-name**:

   ```
   [edit firewall family family]
   user@host# edit filter pm-filter-name
   ```

3. Enable configuration of a firewall filter term **pm-filter-term-name**:

   ```
   [edit firewall family family filter pm-filter-name]
   ```

```
user@host# edit term pm-filter-term-name
```

4. (Optional) Specify the firewall filter match conditions based on the route source address *only if* you want to mirror a subset of the sampled packets.

   - For detailed information about Layer 2 bridging firewall filter match conditions (which are supported on MX Series routers and EX Series switches only), see *Firewall Filter Match Conditions for Layer 2 Bridging Traffic*.
   - For detailed information about VPLS firewall filter match conditions, see *Firewall Filter Match Conditions for VPLS Traffic*.
   - For detailed information about Layer 2 circuit cross-connect (CCC) firewall filter match conditions, see *Firewall Filter Match Conditions for Layer 2 CCC Traffic*.

   NOTE: If you want all sampled packets to be considered to match (and be subjected to the actions specified in the **then** statement), then omit the **from** statement altogether.

5. Enable configuration of the **action** and **action-modifier** to apply to matching packets:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name]
user@host# edit then
```

6. Specify the actions to be taken on matching packets:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set action
```

   The recommended value for the **action** is **accept**. If you do not specify an action, or if you omit the **then** statement entirely, all packets that match the conditions in the **from** statement are accepted.

7. Specify Layer 2 port mirroring or a next-hop group as the **action-modifier**:

   - To reference the Layer 2 port mirroring properties currently in effect for the Packet Forwarding Engine or PIC associated with the underlying physical interface, use the **port-mirror** statement:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set port-mirror
```

- To reference the Layer 2 port mirroring properties configured in a specific named instance, use the port-mirror-instance *pm-instance-name* action modifier:

  ```
  [edit firewall family family filter pm-filter-name term pm-filter-term-name then]
  user@host# set port-mirror-instance pm-instance-name
  ```

  If the underlying physical interface is not bound to a named instance of Layer 2 port mirroring but instead is implicitly bound to the global instance of Layer 2 port mirroring, then traffic at the logical interface is mirrored according to the properties specified in the named instance referenced by the **port-mirror-instance** action modifier.

- To reference a next-hop group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer), use the **next-hop-group** *pm-next-hop-group-name* action modifier:

  ```
  [edit firewall family family filter pm-filter-name term pm-filter-term-name then]
  user@host# set next-hop-group pm-next-hop-group-name
  ```

  For configuration information about next-hop groups, see "Defining a Next-Hop Group for Layer 2 Port Mirroring" on page 1402. If you specify a next-hop group for Layer 2 port mirroring, the firewall filter term applies to the tunnel interface input only.

8. Verify the minimum configuration of the Layer 2 port-mirroring firewall filter:

   ```
   [edit firewall ... ]
   user@host# top
   [edit]
   user@host# show firewall

   family (ethernet-switching | ccc | vpls) { # Type of packets to mirror
     filter pm-filter-name { # Firewall filter name
       term pm-filter-term-name {
         from { # Do not specify match conditions based on route source address
         }
         then {
           action; # Recommended action is 'accept'
           action-modifier; # Three options for Layer 2 port mirroring
         }
       }
     }
   }
   ```

   In the firewall filter term **then** statement, the *action-modifier* can be **port-mirror**, **port-mirror-instance** , or **next-hop-group** *pm-next-hop-group-name*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | 1401

Example: Layer 2 Port Mirroring at a Logical Interface | 1385

Example: Layer 2 Port Mirroring for a Layer 2 VPN | 1391

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394

Example: Layer 2 Port Mirroring to Multiple Destinations | 1412

Configuring Protocol-Independent Firewall Filter for Port Mirroring

On MX Series routers with MPCs, you can configure a firewall filter to mirror Layer 2 and Layer 3 packets at a global level and at an instance level. When port mirror is configured at ingress or egress, the packet entering or exiting an interface is copied and the copies are sent to the local interface for local monitoring.

> **NOTE:** Starting with Junos OS Release 13.3R6, only MPC interfaces support **family any** to do port mirroring. DPC interfaces do not support **family any**.

Typically, the firewall filter is configured such that it mirrors either Layer 2 or Layer 3 packets based on the family configured at the interface. However, in case of an integrated routing and bridging (IRB) interface, Layer 2 packets are not completely mirrored because IRB interfaces are configured to mirror only Layer 3 packets. On such an interface, you can configure a firewall filter and port mirroring parameters in the family **any** to ensure that a packet is completely mirrored irrespective of whether it is a Layer 2 or a Layer 3 packet.

> **NOTE:**
> - For port mirroring at an instance, you can configure one or more families such as **inet**, **inet6**, **ccc**, and **vpls** simultaneously for the same instance.
> - In case of Layer 2 port mirroring, VLAN tags, MPLS headers are retained and can be seen in the mirrored copy at egress.
> - For VLAN normalization, the information before normalization is seen for a mirrored packet at ingress. Similarly, at egress, the information after normalization is seen for the mirrored packet.

Before you begin configuring port mirroring, you must configure valid physical interfaces.

To configure a protocol-independent firewall filter for port mirroring:

1. Configure a global firewall filter for mirroring egress or ingress traffic.

```
[edit firewall family any]
user@host# set filter filter-name {
    term term-name {
        then {
            port-mirror;
            accept;
        }
    }
}
```

2. Configure a firewall filter to mirror traffic for an instance.

```
[edit firewall family any]
user@host# set filter filter-name {
    term term-name {
        then {
            port-mirror-instance instance-name;
            accept;
        }
    }
}
```

3. Configure mirroring parameters for egress and ingress traffic.

```
[edit forwarding-options port-mirroring]
user@host# input {
    maximum-packet-length bytes
    rate rate;
}
family any {
    output {
        (next-hop-group group-name | interface interface-name);
    }
}
```

4. Configure mirroring parameters for an instance. In this configuration, you can specify the output or destination for the Layer 2 packets to be either a valid next-hop group or a Layer 2 interface.

```
[edit forwarding-options port-mirroring]
user@host#instance instance-name {
    family any{
        output {
            (next-hop-group group-name | interface interface-name);
        }
    }
}
```

5. Configure the firewall filter at the ingress or egress interface on which the packets are transmitted.

```
[edit interface interface-name unit]
user@host# filter {
    output filter-name;
    input filter-name;
}
```

Release History Table

Release	Description
13.3R6	Starting with Junos OS Release 13.3R6, only MPC interfaces support **family any** to do port mirroring.

RELATED DOCUMENTATION

Configuring Ethernet Physical Interface Properties

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

Example: Mirroring Employee Web Traffic with a Firewall Filter

IN THIS SECTION

- Requirements | **1352**
- Overview | **1352**

Configuring | 1352
Verification | 1355

Requirements

This example uses the following hardware and software components:

- One switch
- Junos 14.1X53-D20

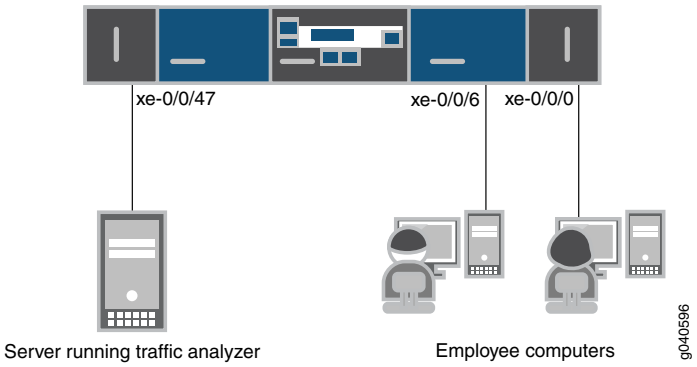
Overview

In this example, **xe-0/0/0** and **xe-0/0/6** serve as connections for employee computers. Interface **xe-0/0/47** is connected to a device running an analyzer application.

Rather than mirror all traffic, it is usually desirable to mirror only certain traffic. This is a more-efficient use of your bandwidth and hardware and might be necessary because of constraints on these assets. This example mirrors only traffic sent from employee computers to the Web.

Figure 52 on page 1352 shows the network topology for this example.

Figure 52: Network Topology for Local Port Mirroring Example



Configuring

To specify that the only traffic that will be mirrored is traffic sent by employees to the Web, perform the tasks explained in this section. To select this traffic for mirroring, you use a firewall filter to specify this traffic and direct it to a port-mirroring instance.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set forwarding-options port-mirroring family inet output interface xe-0/0/47.0 next-hop 192.0.2.100/24
set firewall family inet filter watch-employee term employee-to-corp from destination-address 192.0.2.16/24
set firewall family inet filter watch-employee term employee-to-corp from source-address 192.0.2.16/24
set firewall family inet filter watch-employee term employee-to-corp then accept
set firewall family inet filter watch-employee term employee-to-web from destination-port 80
set firewall family inet filter watch-employee term employee-to-web then port-mirror
set interfaces xe-0/0/0 unit 0 family address 192.0.1.1/24
set interfaces xe-0/0/6 unit 0 family address 192.0.1.2/24
set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
set interfaces xe-0/0/0 unit 0 family inet filter input watch-employee
set interfaces xe-0/0/6 unit 0 family inet filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee to web traffic from the two ports connected to employee computers:

1. Configure a port-mirroring instance, including the output interface and the IP address of the device running the analyzer application as the next hop. (Configure only the output—the input comes from the filter.) You must also specifying that the mirror is for IPv4 traffic (**family inet**).

   ```
   [edit forwarding-options]
   user@switch# set forwarding-options port-mirroring family inet output interface xe-0/0/47.0 next-hop 192.0.2.100/28
   ```

2. Configure an IPv4 (**family inet**) firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the port-mirroring instance. Traffic sent to and arriving from the corporate subnet (destination or source address of **192.0.nn.nn/24**) does not need to be copied, so first create another term to accept that traffic before it reaches the term that sends Web traffic to the instance:

```
[edit firewall family inet]
er@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.nn.nn/24
user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.nn.nn/24
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror
```

3. Configure addresses for the IPv4 interfaces connected to the employee computers and the analyzer device:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet address 192.0.1.1/24
user@switch# set xe-0/0/6 unit 0 family inet address 192.0.1.2/24
user@switch# set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family inet filter input watch-employee
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
    port-mirroring {
        employee-web-monitor {
            output {
                ip-address 192.0.2.100.0;
                }
            }
        }
    }
}
...
firewall family inet {
    filter watch-employee {
        term employee-to-corp {
```

```
            from {
                destination-address 192.0.2.16/24;
                source-address 192.0.2.16/24;
            }
            then accept {
        }
        term employee-to-web {
            from {
                destination-port 80;
            }
            then port-mirror;
        }
    }
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family inet {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family inet {
            filter {
                input watch-employee;
            }
        }
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify that the port mirror analyzer has been configured as expected using the **show forwarding-options port-mirroring** command.

```
user@switch> show forwarding-options port-mirroring
```

```
Instance Name: &global_instance
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    inet                up      xe-0/0/47.0          192.0.2.100
```

Meaning

This output shows that the port-mirroring instance has a ratio of 1 (mirroring every packet, the default setting) and the maximum size of the original packet that was mirrored (**0** indicates the entire packet). If the state of the output interface is down or if the output interface is not configured, the value of state will be **down** and the instance will not be programmed for mirroring.

RELATED DOCUMENTATION

Understanding Port Mirroring | **1183**

Configuring Port Mirroring

Understanding Layer 2 Port Mirroring of PE Router Logical Interfaces

For an MX Series router or an EX Series switch configured as a provider edge (PE) router or PE switch on the customer-facing edge of a service provider network, you can apply a Layer 2 port-mirroring firewall filter at the following ingress and egress points to mirror the traffic between the MX Series router (or an EX Series switch) and customer edge (CE) devices, such as routers and Ethernet switches.

Table 145 on page 1357 describes the ways in which you can apply Layer 2 port-mirroring firewall filters to an MX Series router or an EX Series switch configured as a PE router or PE switch.

Table 145: Application of Layer 2 Port Mirroring Firewall Filters on PE Routers and PE Switches

Point of Application	Scope of Mirroring	Notes	Configuration Details
Ingress Customer-Facing Logical Interface	Packets originating within a service provider customer's network, sent first to a CE device, and sent next to an MX Series router or an EX Series switch acting as a PE router or PE switch.	You can also configure aggregated Ethernet interfaces between CE devices and PE routers or PE switches for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. Traffic received on an aggregated Ethernet interface is forwarded over a different interface based on a lookup of the destination MAC (DMAC) address: • Packets destined for a local site are sent out of the load-balanced child interface. • Packets destined for the remote site are encapsulated and forwarded over a label-switched path (LSP).	See "Applying Layer 2 Port Mirroring to a Logical Interface" on page 1367. For more information about VPLS routing instances, see *Configuring a VPLS Routing Instance* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*.
Egress Customer-Facing Logical Interface	Unicast packets being forwarded by the MX Series router or the EX Series switch to another PE router or PE switch. If you apply a port-mirroring filter to the output for a logical interface, only Unicast packets are mirrored. To mirror Mulitcast, unknown Unicast, and broadcast packets, apply a filter to the input to the flood table of a bridge domain or VPLS routing instance.		See "Applying Layer 2 Port Mirroring to a Logical Interface" on page 1367.

Table 145: Application of Layer 2 Port Mirroring Firewall Filters on PE Routers and PE Switches *(continued)*

Point of Application	Scope of Mirroring	Notes	Configuration Details
Input to a Bridge Domain Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the bridge domain from a CE device.	Forwarding and flood traffic typically consists of broadcast packets, Mulitcast packets, Unicast packets with an unknown destination MAC address, or packets with a MAC entry in the DMAC routing table.	See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain" on page 1370. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.
Input to a VPLS Routing Instance Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the VPLS routing instance from a CE device.		See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance" on page 1373. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Understanding Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces

An aggregated Ethernet interface is a virtual aggregated link that consists of a set of physical interfaces of the same speed and operating in full-duplex link connection mode. You can configure aggregated Ethernet interfaces between CE devices and PE routers for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. If one or more links in the aggregated interface fails, the traffic is switched to the remaining links.

You can apply a Layer 2 port-mirroring firewall filter to an aggregated Ethernet interface to configure port-mirroring at the parent interface. However, if any child interfaces are bound to different Layer 2 port-mirroring instances, packets received at the child interfaces will be mirrored to the destinations specified by their respective port-mirroring instances. Thus, multiple child interfaces can mirror packets to multiple destinations.

For example, suppose the parent aggregated Ethernet interface instance **ae0** has two child interfaces:

- **xe-2/0/0**
- **xe-3/1/2**

Suppose that these child interfaces on **ae0** are bound to two different Layer 2 port-mirroring instances:

- **pm_instance_A**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-2/0/0**.
- **pm_instance_B**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-3/1/2**.

Now suppose you apply a Layer 2 port-mirroring firewall filter to the Layer 2 traffic sent on **ae0.0** (logical unit **0** on the aggregated Ethernet interface instance **0**). This enables port mirroring on **ae0.0**, which has the following effect on the processing of traffic received on the child interfaces for which Layer 2 port-mirroring properties are specified:

- The packets received on **xe-2/0/0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_A**.
- The packets received on **xe-3/1/2.0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_B**.

Because **pm_instance_A** and **pm_instance_B** can specify different packet-selection properties or mirror destination properties, the packets received on **xe-2/0/0** and **xe-3/1/2.0** can mirror different packets to different destinations.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Layer 2 Port Mirroring of PE Router or PE Switch Logical Interfaces

For a router or switch configured as a provider edge (PE) device on the customer-facing edge of a service provider network, you can apply a Layer 2 port-mirroring firewall filter at the following ingress and egress

points to mirror the traffic between the router or switch and customer edge (CE) devices, which are typically also routers and Ethernet switches.

Table 145 on page 1357 describes the ways in which you can apply Layer 2 port-mirroring firewall filters to a router or switch configured as a PE device.

Table 146: Application of Layer 2 Port Mirroring Firewall Filters on PE Devices

Point of Application	Scope of Mirroring	Notes	Configuration Details
Ingress Customer-Facing Logical Interface	Packets originating within a service provider customer's network, sent first to a CE device, and sent next to the PE device.	You can also configure aggregated Ethernet interfaces between CE devices and PE devices for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. Traffic received on an aggregated Ethernet interface is forwarded over a different interface based on a lookup of the destination MAC (DMAC) address: • Packets destined for a local site are sent out of the load-balanced child interface. • Packets destined for the remote site are encapsulated and forwarded over a label-switched path (LSP).	See "Applying Layer 2 Port Mirroring to a Logical Interface" on page 1367. For more information about VPLS routing instances, see *Configuring a VPLS Routing Instance* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*.
Egress Customer-Facing Logical Interface	Unicast packets being forwarded by the PE device to another PE device. **NOTE:** If you apply a port-mirroring filter to the output for a logical interface, only unicast packets are mirrored. To mirror multicast, unknown unicast, and broadcast packets, apply a filter to the input to the flood table of a VLAN or VPLS routing instance.		See "Applying Layer 2 Port Mirroring to a Logical Interface" on page 1367.

Table 146: Application of Layer 2 Port Mirroring Firewall Filters on PE Devices *(continued)*

Point of Application	Scope of Mirroring	Notes	Configuration Details
Input to a VLAN Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the VLAN from a CE device.	Forwarding and flood traffic typically consists of broadcast packets, multicast packets, unicast packets with an unknown destination MAC address, or packets with a MAC entry in the DMAC routing table.	See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain" on page 1370. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.
Input to a VPLS Routing Instance Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the VPLS routing instance from a CE device.		See "Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance" on page 1373. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Layer 2 Port Mirroring of PE Router or PE Switch Aggregated Ethernet Interfaces

An aggregated Ethernet interface is a virtual aggregated link that consists of a set of physical interfaces of the same speed and operating in full-duplex link connection mode. You can configure aggregated Ethernet interfaces between CE devices and PE devices for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. If one or more links in the aggregated interface fails, the traffic is switched to the remaining links.

You can apply a Layer 2 port-mirroring firewall filter to an aggregated Ethernet interface to configure port mirroring at the parent interface. However, if any child interfaces are bound to different Layer 2 port-mirroring instances, packets received at the child interfaces will be mirrored to the destinations specified by their respective port-mirroring instances. Thus, multiple child interfaces can mirror packets to multiple destinations.

For example, suppose the parent aggregated Ethernet interface instance **ae0** has two child interfaces:

- **xe-2/0/0**
- **xe-3/1/2**

Suppose that these child interfaces on **ae0** are bound to two different Layer 2 port-mirroring instances:

- **pm_instance_A**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-2/0/0**.
- **pm_instance_B**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-3/1/2**.

Now suppose you apply a Layer 2 port-mirroring firewall filter to the Layer 2 traffic sent on **ae0.0** (logical unit **0** on the aggregated Ethernet interface instance **0**). This enables port mirroring on **ae0.0**, which has the following effect on the processing of traffic received on the child interfaces for which Layer 2 port-mirroring properties are specified:

- The packets received on **xe-2/0/0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_A**.
- The packets received on **xe-3/1/2.0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_B**.

Because **pm_instance_A** and **pm_instance_B** can specify different packet-selection properties or mirror destination properties, the packets received on **xe-2/0/0** and **xe-3/1/2.0** can mirror different packets to different destinations.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Applying Layer 2 Port Mirroring to a Logical Interface

You can apply a Layer 2 port-mirroring firewall filter to the input or to the output of a logical interface, including an aggregated Ethernet logical interface. Only packets of the address-type family specified by the filter action are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the input to a logical interface or output to a logical interface. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

> **NOTE:** This configuration task shows two Layer 2 port-mirroring firewall filters: one filter applied to the logical interface ingress traffic, and one filter applied to the logical interface egress traffic.

To apply a Layer 2 port-mirroring firewall filter to an input or output logical interface:

1. Configure the underlying physical interface for the logical interface.

   a. Enable configuration of the underlying physical interface:

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

   > **NOTE:** A port-mirroring firewall filter can also be applied to an aggregated-Ethernet logical interface.

   b. For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface:

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

   c. For 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, set the logical link-layer encapsulation type:

```
[edit interfaces interface-name]
user@host# set encapsulation extended-vlan-ethernet-switching
```

2. Configure the logical interface to which you want to apply a Layer 2 port-mirroring firewall filter.

   a. Specify the logical unit number:

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

   b. For a Fast Ethernet, Gigabit Ethernet, or Aggregated Ethernet interface, bind an 802.1Q VLAN tag ID to the logical interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set vlan-id number
   ```

3. Enable specification of an input or output filter to be applied to Layer 2 packets that are part of bridging domain, Layer 2 switching cross-connects, or virtual private LAN service (VPLS).

   - If the filter is to be evaluated when packets are received on the interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set family family filter input pm-filter-name-a
   ```

   - If the filter is to be evaluated when packets are sent on the interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set family family filter output pm-filter-name-b
   ```

   The value of the *family* option can be **ethernet-switching**, **ccc**, or **vpls**.

   NOTE: If port-mirroring firewall filters are applied at both the input and output of a logical interface, two copies of each packet are mirrored. To prevent the router or switch from forwarding duplicate packets to the same destination, include the optional **mirror-once** statement at the **[edit forwarding-options]** hierarchy level.

4. Verify the minimum configuration for applying a named Layer 2 port mirroring firewall filter to a logical interface:

```
[edit interfaces interface-name unit logical-unit-number family family filter ... ]
user@host# top
[edit]
user@host# show interfaces

interfaces {
    interface-name {
        vlan-tagging;
        encapsulation extended-vlan-ethernet-switching;
        unit number { # Apply a filter to the input of this interface
            vlan-id number;
            family (ethernet-switching | ccc | vpls) {
                filter {
                    input pm-filter-for-logical-interface-input;
                }
            }
        }
        unit number { # Apply a filter to the output of this interface
            vlan-id number;
            family (ethernet-switching | ccc | vpls) {
                filter {
                    output pm-filter-for-logical-interface-output;
                }
            }
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | 1370

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | 1373

Example: Layer 2 Port Mirroring at a Logical Interface | 1385

Example: Layer 2 Port Mirroring for a Layer 2 VPN | 1391

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394

Applying Layer 2 Port Mirroring to a Logical Interface

You can apply a Layer 2 port-mirroring firewall filter to the input or to the output of a logical interface, including an aggregated Ethernet logical interface. Only packets of the address-type family specified by the filter action are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the input to a logical interface or output to a logical interface. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

> **NOTE:** This configuration task shows two Layer 2 port-mirroring firewall filters: one filter applied to the logical interface ingress traffic, and one filter applied to the logical interface egress traffic.

To apply a Layer 2 port-mirroring firewall filter to an input or output logical interface:

1. Configure the underlying physical interface for the logical interface.

   a. Enable configuration of the underlying physical interface:

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

   > **NOTE:** A port-mirroring firewall filter can also be applied to an aggregated-Ethernet logical interface.

   b. For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface:

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

   c. For 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, set the logical link-layer encapsulation type:

```
[edit interfaces interface-name]
user@host# set encapsulation extended-vlan-bridge
```

2. Configure the logical interface to which you want to apply a Layer 2 port-mirroring firewall filter.

   a. Specify the logical unit number:

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

   b. For a Fast Ethernet, Gigabit Ethernet, or Aggregated Ethernet interface, bind an 802.1Q VLAN tag ID to the logical interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set vlan-id number
   ```

3. Enable specification of an input or output filter to be applied to Layer 2 packets that are part of bridging domain, Layer 2 switching cross-connects, or virtual private LAN service (VPLS).

   - If the filter is to be evaluated when packets are received on the interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set family family filter input pm-filter-name-a
   ```

   - If the filter is to be evaluated when packets are sent on the interface:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set family family filter output pm-filter-name-b
   ```

   The value of the *family* option can be **bridge**, **ccc**, or **vpls**.

   NOTE: If port-mirroring firewall filters are applied at both the input and output of a logical interface, two copies of each packet are mirrored. To prevent the router from forwarding duplicate packets to the same destination, include the optional **mirror-once** statement at the **[edit forwarding-options]** hierarchy level.

4. Verify the minimum configuration for applying a named Layer 2 port-mirroring firewall filter to a logical interface:

```
[edit interfaces interface-name unit logical-unit-number family family filter ... ]
user@host# top
[edit]
user@host# show interfaces

interfaces {
    interface-name {
        vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit number { # Apply a filter to the input of this interface
            vlan-id number;
            family (bridge | ccc | vpls) {
                filter {
                    input pm-filter-for-logical-interface-input;
                }
            }
        }
        unit number { # Apply a filter to the output of this interface
            vlan-id number;
            family (bridge | ccc | vpls) {
                filter {
                    output pm-filter-for-logical-interface-output;
                }
            }
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | 1370

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | 1373

Example: Layer 2 Port Mirroring at a Logical Interface | 1385

Example: Layer 2 Port Mirroring for a Layer 2 VPN | 1391

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a bridge domain. Only packets of the specified family type and forwarded or flooded to that bridge domain are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a bridge domain or flooded to a bridge domain. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

  NOTE: This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the bridge domain forwarding table ingress traffic, and one filter applied to the bridge domain flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a bridge domain:

1. Enable configuration of the bridge domain *bridge-domain-name* to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

   - For a bridge domain:

     ```
     [edit]
     user@host# edit bridge-domains bridge-domain-name
     ```

   - For a bridge domain under a routing instance:

     ```
     [edit]
     user@host# edit routing-instances routing-instance-name bridge-domains bridge-domain-name
     user@host# set instance-type virtual-switch
     ```

   For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Configure the bridge domain:

   ```
   [edit]
   ```

```
user@host# set domain-type bridge
user@host# set interface interface-name
user@host# set routing-interface routing-interface-name
```

For detailed configuration information, see *Configuring a Bridge Domain* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*.

3. Enable configuration of traffic forwarding on the bridge domain:

```
[edit ... bridge-domains bridge-domain-name]
user@host# edit forwarding-options
```

4. Apply a Layer 2 port-mirroring firewall filter to the bridge domain forwarding table or flood table.

   - To mirror packets being forwarded to the bridge domain:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set filter input pm-filter-for-bd-ingress-forwarded
```

   - To mirror packets being flooded to the bridge domain:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
```

```
user@host# set flood input pm-filter-for-bd-ingress-flooded
```

5. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the bridge domain.

   a. Navigate to the hierarchy level at which the bridge domain is configured:

      - **[edit]**
      - **[edit routing-instances *routing-instance-name*]**

   b. Display the bridge domain configurations:

```
user@host# show bridge domains

bridge-domains {
    bridge-domain-name {
        instance-type virtual-switch; # For a bridge domain under a routing instance.
        domain-type bridge;
        interface interface-name;
        forwarding-options {
            filter { # Mirror ingress forwarded traffic
                input pm-filter-for-bd-ingress-forwarded;
            }
            flood { # Mirror ingress flooded traffic
                input pm-filter-for-bd-ingress-flooded;
            }
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Applying Layer 2 Port Mirroring to a Logical Interface | **1367**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1373**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a VPLS routing instance. Only packets of the specified family type and forwarded or flooded to that VPLS routing instance are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a VPLS routing instance or flooded to a bridge domain. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

  NOTE: This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the VPLS routing instance forwarding table ingress traffic, and one filter applied to the VPLS routing instance flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a VPLS routing instance:

1. Enable configuration of the VPLS routing instance to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

   ```
   [edit]
   user@host# edit routing-instances routing-instance-name
   user@host# set instance-type vpls
   user@host# set interface interface-name
   user@host# set route-distinguisher (as-number:number | ip-address:number)
   user@host# set vrf-import [policy-names]
   user@host# set vrf-export [policy-names]
   user@host# edit protocols vpls
   user@host@ ... vpls-configuration ...
   ```

   For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Enable configuration of traffic forwarding on the VPLS routing instance:

```
[edit routing-instances routing-instance-name protocols vpls]
user@host# up 2
[edit routing-instances routing-instance-name]
user@host# edit forwarding-options
```

3. Apply a Layer 2 port-mirroring firewall filter to the VPLS routing instance forwarding table or flood table.

   - To mirror packets being forwarded to the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set filter input pm-filter-for-vpls-ri-forwarded
```

   - To mirror packets being flooded to the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set flood input pm-filter-for-vpls-ri-flooded
```

4. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# top
[edit]
user@host# show routing-instances

routing-instances {
    routing-instance-name {
        instance-type vpls;
        interface interface-name;
        route-distinguisher (as-number:number | ip-address:number);
        vrf-import [policy-names];
        vrf-export [policy-names];
        protocols {
            vpls {
                ...vpls-configuration...
            }
        }
        forwarding-options {
            family vpls {
```

```
            filter { # Mirror ingress forwarded traffic
                input pm-filter-for-vpls-ri-forwarded;
            }
            flood { # Mirror ingress flooded traffic
                input pm-filter-for-vpls-ri-flooded;
            }
        }
    }
  }
}
```

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | **1200**
- *Layer 2 Port Mirroring Firewall Filters*
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**
- Applying Layer 2 Port Mirroring to a Logical Interface | **1367**
- Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | **1370**
- Example: Layer 2 Port Mirroring at a Logical Interface | **1385**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a VPLS routing instance. Only packets of the specified family type and forwarded or flooded to that VPLS routing instance are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a VPLS routing instance or flooded to a VLAN. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

> **NOTE:** This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the VPLS routing instance forwarding table ingress traffic, and one filter applied to the VPLS routing instance flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a VPLS routing instance:

1. Enable configuration of the VPLS routing instance to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

```
[edit]
user@host# edit routing-instances routing-instance-name
user@host# set instance-type vpls
user@host# set interface interface-name
user@host# set route-distinguisher (as-number:number | ip-address:number)
user@host# set vrf-import [policy-names]
user@host# set vrf-export [policy-names]
user@host# edit protocols vpls
user@host@ ... vpls-configuration ...
```

   For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Enable configuration of traffic forwarding on the VPLS routing instance:

```
[edit routing-instances routing-instance-name protocols vpls]
user@host# up 2
[edit routing-instances routing-instance-name]
user@host# edit forwarding-options
```

3. Apply a Layer 2 port-mirroring firewall filter to the VPLS routing instance forwarding table or flood table.

   - To mirror packets being forwarded to the VPLS routing instance:

     ```
     [edit routing-instances routing-instance-name forwarding-options]
     user@host# set filter input pm-filter-for-vpls-ri-forwarded
     ```

   - To mirror packets being flooded to the VPLS routing instance:

     ```
     [edit routing-instances routing-instance-name forwarding-options]
     user@host# set flood input pm-filter-for-vpls-ri-flooded
     ```

4. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the VPLS routing instance:

   ```
   [edit routing-instances routing-instance-name forwarding-options]
   user@host# top
   [edit]
   user@host# show routing-instances

   routing-instances {
       routing-instance-name {
           instance-type vpls;
           interface interface-name;
           route-distinguisher (as-number:number | ip-address:number);
           vrf-import [policy-names];
           vrf-export [policy-names];
           protocols {
               vpls {
                   ...vpls-configuration...
               }
           }
           forwarding-options {
               family vpls {
                   filter { # Mirror ingress forwarded traffic
                       input pm-filter-for-vpls-ri-forwarded;
                   }
                   flood { # Mirror ingress flooded traffic
                       input pm-filter-for-vpls-ri-flooded;
                   }
               }
           }
       }
   ```

```
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Applying Layer 2 Port Mirroring to a Logical Interface | **1367**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain | **1370**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | **1394**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VLAN

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a VLAN. Only packets of the specified family type and forwarded or flooded to that VLAN are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a VLAN or flooded to a VLAN. For details, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

> **NOTE:** This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the VLAN forwarding table ingress traffic, and one filter applied to the VLAN flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a VLAN:

1. Enable configuration of the VLAN ***bridge-domain-name*** to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

   - For a VLAN:

     ```
     [edit]
     user@host# edit bridge-domains bridge-domain-name
     ```

   - For a VLAN under a routing instance:

     ```
     [edit]
     user@host# edit routing-instances routing-instance-name bridge-domains bridge-domain-name
     user@host# set instance-type virtual-switch
     ```

     For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Configure the VLAN:

   ```
   [edit]
   user@host# set domain-type bridge
   user@host# set interface interface-name
   user@host# set routing-interface routing-interface-name
   ```

   For more detailed configuration information, see *Configuring a Bridge Domain* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*.

3. Enable configuration of traffic forwarding on the VLAN:

```
[edit ... bridge-domains bridge-domain-name]
user@host# edit forwarding-options
```

4. Apply a Layer 2 port-mirroring firewall filter to the VLAN forwarding table or flood table.

   - To mirror packets being forwarded to the VLAN:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set filter input pm-filter-for-bd-ingress-forwarded
```

   - To mirror packets being flooded to the VLAN:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
```

```
user@host# set flood input pm-filter-for-bd-ingress-flooded
```

5. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the VLAN.

   a. Navigate to the hierarchy level at which the VLAN is configured:

      - **[edit]**
      - **[edit routing-instances *routing-instance-name*]**

   b. Display the VLAN configurations:

```
user@host# show vlans

vlans {
    vlan-name {
        instance-type virtual-switch; # For a bridge domain under a routing instance.
        domain-type bridge;
        interface interface-name;
        forwarding-options {
            filter { # Mirror ingress forwarded traffic
                input pm-filter-for-bd-ingress-forwarded;
            }
            flood { # Mirror ingress flooded traffic
                input pm-filter-for-bd-ingress-flooded;
            }
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Applying Layer 2 Port Mirroring to a Logical Interface | **1367**

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance | **1373**

Example: Layer 2 Port Mirroring at a Logical Interface | **1385**

Example: Layer 2 Port Mirroring for a Layer 2 VPN | **1391**

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links | 1394

Example: Layer 2 Port Mirroring at a Logical Interface

The following steps describe an example in which the global port-mirroring instance and a port-mirroring firewall filter are used to configure Layer 2 port mirroring for the input to a logical interface.

1. Configure the VLAN **example-bd-with-analyzer**, which contains the external packet analyzer, and the VLAN **example-bd-with-traffic**, which contains the source and destination of the Layer 2 traffic being mirrored:

```
[edit]
bridge-domains {
   example-bd-with-analyzer { # Contains an external traffic analyzer
      vlan-id 1000;
      interface ge-2/0/0.0; # External analyzer
   }
   example-bd-with-traffic { # Contains traffic input and output interfaces
      vlan-id 1000;
      interface ge-2/0/6.0; # Traffic input port
      interface ge-3/0/1.2; # Traffic output port
   }
}
```

   Assume that logical interface **ge-2/0/0.0** is associated with an external traffic analyzer that is to receive port-mirrored packets. Assume that logical interfaces **ge-2/0/6.0** and **ge-3/0/1.2** will be traffic input and output ports, respectively.

2. Configure Layer 2 port-mirroring for the global instance, with the port-mirroring destination being the VLAN interface associated with the external analyzer (logical interface **ge-2/0/0.0** on VLAN **example-bd-with-analyzer**). Be sure to enable the option that allows filters to be applied to this port-mirroring destination:

```
[edit]
forwarding-options {
   port-mirroring {
      input {
         rate 10;
         run-length 5;
      }
      family ethernet-switching {
```

```
        output {
            interface ge-2/0/0.0; # Mirror packets to the external analyzer
            no-filter-check; # Allow filters on the mirror destination interface
        }
    }
  }
}
```

The **input** statement at the **[edit forwarding-options port-mirroring]** hierarchy level specifies that sampling begins every tenth packet and that each of the first five packets selected are to be mirrored.

The **output** statement at the **[edit forwarding-options port-mirroring family ethernet-switching]** hierarchy level specifies the output mirror interface for Layer 2 packets in a bridging environment:

- Logical interface **ge-2/0/0.0**, which is associated with the external packet analyzer, is configured as the port-mirroring destination.
- The optional **no-filter-check** statement allows filters to be configured on this destination interface.

3. Configure the Layer 2 port-mirroring firewall filter **example-bridge-pm-filter**:

```
[edit]
firewall {
  family ethernet-switching {
    filter example-bridge-pm-filter {
      term example-filter-terms {
        then {
          accept;
          port-mirror;
        }
      }
    }
  }
}
```

When this firewall filter is applied to the input or output of a logical interface for traffic in a bridging environment, Layer 2 port mirroring is performed according to the input packet-sampling properties and mirror destination properties configured for the Layer 2 port mirroring global instance. Because this firewall filter is configured with the single, default filter action **accept**, all packets selected by the **input** properties (**rate** = **10** and **run-length** = **5**) match this filter.

4. Configure the logical interfaces:

```
[edit]
```

```
interfaces {
    ge-2/0/0 { # Define the interface to the external analyzer
        encapsulation ethernet-bridge;
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-2/0/6 { # Define the traffic input port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 0 {
            vlan-id 100;
            family ethernet-switching {
                filter {
                    input example-bridge-pm-filter; # Apply the port-mirroring firewall filter
                }
            }
        }
    }
    ge-3/0/1 { # Define the traffic output port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 2 {
            vlan-tags outer 10 inner 20;
            family ethernet-switching;
        }
    }
}
```

Packets received at logical interface **ge-2/0/6.0** on VLAN **example-bd-with-traffic** are evaluated by the port-mirroring firewall filter **example-bridge-pm-filter**. The firewall filter acts on the input traffic according to the filter actions configured in the firewall filter itself plus the input packet-sampling properties and mirror destination properties configured in the global port-mirroring instance:

- All packets received at **ge-2/0/6.0** are forwarded to their (assumed) normal destination at logical interface **ge-3/0/1.2**.
- For every ten input packets, copies of the first five packets in that selection are forwarded to the external analyzer at logical interface **ge-0/0/0.0** in the other VLAN, **example-bd-with-analyzer**.

If you configure the port-mirroring firewall filter **example-bridge-pm-filter** to take the **discard** action instead of the **accept** action, all original packets are discarded while copies of the packets selected using the global port-mirroring **input** properties are sent to the external analyzer.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Example: Layer 2 Port Mirroring at a Logical Interface

The following steps describe an example in which the global port-mirroring instance and a port-mirroring firewall filter are used to configure Layer 2 port mirroring for the input to a logical interface.

1. Configure the bridge domain **example-bd-with-analyzer**, which contains the external packet analyzer, and the bridge domain **example-bd-with-traffic**, which contains the source and destination of the Layer 2 traffic being mirrored:

```
[edit]
bridge-domains {
   example-bd-with-analyzer { # Contains an external traffic analyzer
      vlan-id 1000;
      interface ge-2/0/0.0; # External analyzer
   }
   example-bd-with-traffic { # Contains traffic input and output interfaces
      vlan-id 1000;
      interface ge-2/0/6.0; # Traffic input port
      interface ge-3/0/1.2; # Traffic output port
   }
}
```

   Assume that logical interface **ge-2/0/0.0** is associated with an external traffic analyzer that is to receive port-mirrored packets. Assume that logical interfaces **ge-2/0/6.0** and **ge-3/0/1.2** will be traffic input and output ports, respectively.

2. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/0/0.0** on bridge domain **example-bd-with-analyzer**). Be sure to enable the option that allows filters to be applied to this port-mirroring destination:

```
[edit]
forwarding-options {
   port-mirroring {
      input {
```

```
            rate 10;
            run-length 5;
        }
        family bridge {
            output {
                interface ge-2/0/0.0; # Mirror packets to the external analyzer
                no-filter-check; # Allow filters on the mirror destination interface
            }
        }
    }
}
```

The **input** statement at the **[edit forwarding-options port-mirroring]** hierarchy level specifies that sampling begins every tenth packet and that each of the first five packets selected are to be mirrored.

The **output** statement at the **[edit forwarding-options port-mirroring family bridge]** hierarchy level specifies the output mirror interface for Layer 2 packets in a bridging environment:

- Logical interface **ge-2/0/0.0**, which is associated with the external packet analyzer, is configured as the port-mirroring destination.
- The optional **no-filter-check** statement allows filters to be configured on this destination interface.

3. Configure the Layer 2 port-mirroring firewall filter **example-bridge-pm-filter**:

```
[edit]
firewall {
    family bridge {
        filter example-bridge-pm-filter {
            term example-filter-terms {
                then {
                    accept;
                    port-mirror;
                }
            }
        }
    }
}
```

When this firewall filter is applied to the input or output of a logical interface for traffic in a bridging environment, Layer 2 port mirroring is performed according to the input packet-sampling properties and mirror destination properties configured for the Layer 2 port mirroring global instance. Because this firewall filter is configured with the single, default filter action **accept**, all packets selected by the **input** properties (**rate** = **10** and **run-length** = **5**) match this filter.

4. Configure the logical interfaces:

```
[edit]
interfaces {
    ge-2/0/0 { # Define the interface to the external analyzer
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
    ge-2/0/6 { # Define the traffic input port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 0 {
            vlan-id 100;
            family bridge {
                filter {
                    input example-bridge-pm-filter; # Apply the port-mirroring firewall filter
                }
            }
        }
    }
    ge-3/0/1 { # Define the traffic output port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 2 {
            vlan-tags outer 10 inner 20;
            family bridge;
        }
    }
}
```

Packets received at logical interface **ge-2/0/6.0** on bridge domain **example-bd-with-traffic** are evaluated by the port-mirroring firewall filter **example-bridge-pm-filter**. The firewall filter acts on the input traffic according to the filter actions configured in the firewall filter itself plus the input packet-sampling properties and mirror destination properties configured in the global port-mirroring instance:

- All packets received at **ge-2/0/6.0** are forwarded to their (assumed) normal destination at logical interface **ge-3/0/1.2**.
- For every ten input packets, copies of the first five packets in that selection are forwarded to the external analyzer at logical interface **ge-0/0/0.0** in the other bridge domain, **example-bd-with-analyzer**.

If you configure the port-mirroring firewall filter **example-bridge-pm-filter** to take the **discard** action instead of the **accept** action, all original packets are discarded while copies of the packets selected using the global port-mirroring **input** properties are sent to the external analyzer.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Example: Layer 2 Port Mirroring for a Layer 2 VPN

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc**.

1. Configure the VLAN **port-mirror-bd**, which contains the external packet analyzer:

```
[edit]
vlans {
    port-mirror-vlan { # Contains an external traffic analyzer
        interface ge-2/2/9.0; # External analyzer
    }
}
```

2. Configure the Layer 2 VPN CCC to connect logical interface **ge-2/0/1.0** and logical interface **ge-2/0/1.1**:

```
[edit]
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ge-2/0/1.0;
            interface ge-2/0/1.1;
        }
    }
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the VLAN interface associated with the external analyzer (logical interface **ge-2/2/9.0** on VLAN **example-bd-with-analyzer**):

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/9.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            inst1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
                family ccc {
                    output {
                        interface ge-2/2/9.0;
                    }
                {
            }
        }
    }
}
```

4. Define the Layer 2 port-mirroring firewall filter **pm_filter_ccc** for **family ccc**:

```
[edit]
firewall {
    family ccc {
        filter pm_filter_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
```

```
}
```

5. Apply the port mirror instance to the chassis:

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance inst1;
    }
}
```

6. Configure interface **ge-2/2/9** for the VLANs, and configure interface **ge-2/0/1** for port mirroring with the **pm_filter_ccc** firewall filter:

```
[edit]
interfaces {
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-2/0/1 {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_filter_ccc;
                }
            }
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_filter_ccc;
                }
            }
        }
    }
```

```
}
```

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | 1200
- *Layer 2 Port Mirroring Firewall Filters*
- Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Example: Layer 2 Port Mirroring for a Layer 2 VPN

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc**.

1. Configure the bridge domain **port-mirror-bd**, which contains the external packet analyzer:

```
[edit]
bridge-domains {
   port-mirror-bd { # Contains an external traffic analyzer
      interface ge-2/2/9.0; # External analyzer
   }
}
```

2. Configure the Layer 2 VPN CCC to connect logical interface **ge-2/0/1.0** and logical interface **ge-2/0/1.1**:

```
[edit]
protocols {
   mpls {
      interface all;
   }
   connections {
      interface-switch if_switch {
         interface ge-2/0/1.0;
         interface ge-2/0/1.1;
      }
   }
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/2/9.0** on bridge domain **example-bd-with-analyzer**):

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/9.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            inst1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
                family ccc {
                    output {
                        interface ge-2/2/9.0;
                    }
                {
            }
        }
    }
}
```

4. Define the Layer 2 port-mirroring firewall filter **pm_filter_ccc** for **family ccc**:

```
[edit]
firewall {
    family ccc {
        filter pm_filter_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
```

```
}
```

5. Apply the port mirror instance to the chassis:

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance inst1;
    }
}
```

6. Configure interface **ge-2/2/9** for the VLANs, and configure interface **ge-2/0/1** for port mirroring with the **pm_filter_ccc** firewall filter:

```
[edit]
interfaces {
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
    ge-2/0/1 {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_filter_ccc;
                }
            }
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_filter_ccc;
                }
            }
        }
    }
```

```
}
```

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | 1200
- *Layer 2 Port Mirroring Firewall Filters*
- Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc** and aggregated Ethernet links.

1. Configure the bridge domain **port_mirror_bd**, which contains the external packet analyzer:

```
[edit]
bridge-domains {
   port_mirror_bd { # Contains an external traffic analyzer
      interface ge-2/2/8.0; # External analyzer
   }
}
```

2. Configure the Layer 2 VPN CCC to connect interface **ae0.0** and interface **ae0.1**:

```
[edit]
protocols {
   mpls {
      interface all;
   }
   connections {
      interface-switch if_switch {
         interface ae0.0;
         interface ae0.1;
      }
   }
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/2/9.0** on bridge domain **example_bd_with_analyzer**):

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/8.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            pm_instance_1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
                family ccc {
                    output {
                        interface ge-2/2/8.0;
                    }
                {
            }
        }
    }
}
```

4. Configure the firewall filter **pm_ccc** for **family ccc**:

```
[edit]
firewall {
    family ccc {
        filter pm_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
```

```
}
```

5. Apply the aggregated Ethernet interfaces and port mirror instance to the chassis:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 10;
        }
    }
    fpc 2 {
        port-mirror-instance pm_instance_1;
    }
}
```

6. Configure interfaces **ae0** and **ge-2/0/2** (for aggregated Ethernet) and **ge-2/2/8** (for port mirroring) with the **pm_ccc** filter:

```
[edit]
interfaces {
    ae0 {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_ccc;
                }
            }
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_ccc;
                }
            }
        }
    }
    ge-2/0/2 {
```

```
        gigether-options {
            802.3ad ae0;
        }
    }
    ge-2/2/8 {
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc** and aggregated Ethernet links.

1. Configure the VLAN **port_mirror_bd**, which contains the external packet analyzer:

```
[edit]
vlans {
    port_mirror_vlan { # Contains an external traffic analyzer
        interface ge-2/2/8.0; # External analyzer
    }
}
```

2. Configure the Layer 2 VPN CCC to connect interface **ae0.0** and interface **ae0.1**:

```
[edit]
protocols {
    mpls {
```

```
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ae0.0;
            interface ae0.1;
        }
    }
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the VLAN interface associated with the external analyzer (logical interface **ge-2/2/9.0** on VLAN **example_bd_with_analyzer**):

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/8.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            pm_instance_1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
                family ccc {
                    output {
                        interface ge-2/2/8.0;
                    }
                {
            }
        }
    }
}
```

4. Configure the firewall filter **pm_ccc** for **family ccc**:

```
[edit]
firewall {
    family ccc {
        filter pm_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
}
```

5. Apply the aggregated Ethernet interfaces and port mirror instance to the chassis:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 10;
        }
    }
    fpc 2 {
        port-mirror-instance pm_instance_1;
    }
}
```

6. Configure interfaces **ae0** and **ge-2/0/2** (for aggregated Ethernet) and **ge-2/2/8** (for port mirroring) with the **pm_ccc** filter:

```
[edit]
interfaces {
    ae0 {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_ccc;
                }
            }
```

```
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_ccc;
                }
            }
        }
    }
    ge-2/0/2 {
        gigether-options {
            802.3ad ae0;
        }
    }
    ge-2/2/8 {
        encapsulation ethernet-bridge;
        unit 0 {
            family ethernet-switching;
        }
    }
}
```

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**

Layer 2 Port Mirroring Firewall Filters

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

CHAPTER 40

Configuring Port Mirroring for Multiple Destinations

IN THIS CHAPTER

- Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | **1401**
- Defining a Next-Hop Group for Layer 2 Port Mirroring | **1402**
- Defining a Next-Hop Group on MX Series Routers for Port Mirroring | **1404**
- Example: Configuring Multiple Port Mirroring with Next-Hop Groups on M, MX and T Series Routers | **1407**
- Example: Layer 2 Port Mirroring to Multiple Destinations | **1412**

Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups

On an MX Series router and on an EX Series switch, you can mirror traffic to multiple destinations by configuring next-hop groups in Layer 2 port-mirroring firewall filters applied to tunnel interfaces. The mirroring of packets to multiple destinations is also known as *multipacket port mirroring*,

> **NOTE:** Junos OS Release 9.5 introduced support for Layer 2 port mirroring using next-hop groups on MX Series routers, but required installation of a Tunnel PIC. Beginning in Junos OS Release 9.6, Layer 2 port mirroring using next-hop groups on MX Series routers does not require Tunnel PICs.

On MX Series routers and on EX Series switches, you can define a firewall filter for mirroring packets to a next-hop group. The next-hop group can contain Layer 2 members, Layer 3 members, and subgroups that are either unit list (mirroring packets to each interface) or load-balanced (mirroring packets to one of several interfaces). The MX Series router and the EX Series switch supports up to 30 next-hop groups. Each next-hop group supports up to 16 next-hop addresses. Each next-hop group must specify at least two addresses.

To enable port mirroring to the members of a next-hop group, you specify the next-hop group as the filter action of a firewall filter, and then you apply the firewall filter to logical tunnel interfaces (**lt-**) or virtual tunnel interfaces (**vt-**) on the MX Series router or on the EX Series switch.

NOTE: The use of subgroups for load-balancing mirrored traffic is not supported.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | **1200**Understanding Layer 2 Port Mirroring | **1200**

Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**

Defining a Next-Hop Group for Layer 2 Port Mirroring | **1402**

Example: Layer 2 Port Mirroring to Multiple Destinations | **1412**

Defining a Next-Hop Group for Layer 2 Port Mirroring

On MX Series routers and EX Series switches, you can mirror tunnel interface input traffic to multiple destinations. To this form of *multipacket port mirroring*, you specify two or more additional destinations in a next-hop group, define a firewall filter that references the next-hop group as the filter action, and then apply the filter to a logical tunnel interface (**lt-**) or virtual tunnel interfaces (**vt-**) on the MX Series router and on an EX Series switch.

NOTE: This topic describes how to define a next-hop group for Layer 2 port mirroring to multiple destinations. For detailed information about defining a firewall filter for Layer 2 port mirroring to multiple destinations, see "Defining a Layer 2 Port-Mirroring Firewall Filter" on page 1343.

To define a next-hop group for a Layer 2 port-mirroring firewall filter action:

1. Enable configuration of Layer 2 forwarding options.

   - To enable Layer 2 forwarding options at the top level:

     ```
     [edit]
     user@host edit forwarding-options port-mirroring family (ccc | vpls) output
     ```

   - To enable Layer 2 forwarding options for a routing instance:

     ```
     [edit]
     user@host edit forwarding-options port-mirroring instance instance-name family (ccc | vpls) output
     ```

2. Enable configuration of a next-hop-group for Layer 2 port mirroring:

   ```
   [edit forwarding-options port-mirroring ... family (ccc | vpls) output]
   user@host# edit next-hop-group pm-next-hop-group-name
   ```

3. Specify the type of addresses to be used in the next-hop group configuration. By default, the next-hop group is specified using Layer 3 addresses (**group-type inet**). To specify the next-hop group using Layer 2 addresses instead, you must include the **group-type layer-2** statement:

   ```
   [edit forwarding-options port-mirroring ... family (ccc | vpls) output next-hop-group pm-next-hop-group-name]
   user@host# set group-type layer-2
   ```

4. Specify the logical interfaces of the next-hop route (or switch):

   ```
   [edit forwarding-options port-mirroring ... family (ccc | vpls) output next-hop-group pm-next-hop-group-name]
   user@host# set interface logical-interface-name-1
   user@host# set interface logical-interface-name-2
   ```

   The MX Series router and the EX Series switch supports up to 30 next-hop groups. Each next-hop group supports up to 16 next-hop addresses. Each next-hop group must specify at least two addresses.

5. Verify the configuration of the next-hop group:

   ```
   [edit forwarding-options port-mirroring ... family (ccc | vpls) output next-hop-group pm-next-hop-group-name]
   user@host# top
   [edit]
   ```

```
user@host# show forwarding-options

...
next-hop-group pm-next-hop-group-name { # Next-hop group on a bridge domain.
    group-type layer-2;
    interface logical-interface-name-1;
    interface logical-interface-name-2;
}
...
```

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | 1200
- Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | 1401
- Defining a Layer 2 Port-Mirroring Firewall Filter | 1343
- Displaying Next-Hop Group Settings and Status | 1457
- Example: Layer 2 Port Mirroring to Multiple Destinations | 1412

Defining a Next-Hop Group on MX Series Routers for Port Mirroring

Starting with release 14.2, on routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

You can configure simultaneous use of sampling and port mirroring, and set an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both sampling and port mirroring, only one action can be performed, and port mirroring takes precedence. For example, if you configure an interface to sample every packet input to the interface and a filter also selects the packet to be port mirrored to another interface, only the port mirroring takes effect. All other packets not matching the explicit filter port-mirroring criteria continue to be sampled when forwarded to their final destination.

Next-hop groups allow you to include port mirroring on multiple interfaces.

On MX Series routers, you can mirror tunnel interface input traffic to multiple destinations. To this form of multipacket port mirroring, you specify two or more destinations in a next-hop group, define a firewall filter that references the next-hop group as the filter action, and then apply the filter to a logical tunnel interface **lt-**) or virtual tunnel interfaces (**vt-** on the MX Series router.

To define a next-hop group for a Layer 2 port-mirroring firewall filter action:

1. Enable the configuration of forwarding options.

   ```
   [edit]
   user@host set forwarding-options port-mirroring family (inet | inet6) output
   ```

2. Enable configuration of a next-hop-group for Layer 2 port mirroring.

   ```
   [edit forwarding-options port-mirroring ... family (inet | inet6) output]
   user@host# set next-hop-group next-hop-group-name
   ```

3. Specify the type of addresses to be used in the next-hop group configuration.

   ```
   [edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-hop-group-name]
   user@host# set group-type inet6
   ```

4. Specify the interfaces of the next-hop route.

   ```
   [edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-hop-group-name]
   user@host# set interface logical-interface-name-1
   user@host# set interface logical-interface-name-2
   ```

   or

   ```
   [edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-hop-group-name]
   user@host# set interface interface-name next-hop next-hop-address
   ```

   The MX Series router supports up to 30 next-hop groups. Each next-hop group supports up to 16 next-hop addresses. Each next-hop group must specify at least two addresses. The *next-hop-address* can be an IPv4 or IPv6 address.

5. (Optional) Specify the next-hop subgroup.

   ```
   [edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-hop-group-name]
   user@host# set next-hop-subgroup subgroup-name interface interface-name next-hop next-hop-address
   ```

6. Verify the configuration of the next-hop group.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-hop-group-name]
user@host# top
[edit]
user@host# show forwarding-options

...
next-hop-group next-hop-group-name {
    group-type inet6;
    interface logical-interface-name-1;
    interface interface-name{
        next-hop next-hop-address;
    }
    next-hop-subgroup subgroup-name{
        interface interface-name{
            next-hop next-hop-address;
        }
    }
}
...
```

Release History Table

Release	Description
14.2	Starting with release 14.2, on routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis.

RELATED DOCUMENTATION

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

Example: Configuring Multiple Port Mirroring with Next-Hop Groups on M, MX and T Series Routers | **1407**

Example: Configuring Multiple Port Mirroring with Next-Hop Groups on M, MX and T Series Routers

When you need to analyze traffic containing more than one packet type, or you wish to perform multiple types of analysis on a single type of traffic, you can implement multiple port mirroring and next-hop groups. You can make up to 16 copies of traffic per group and send the traffic to next-hop group members. A maximum of 30 groups can be configured on a router at any given time. The port-mirrored traffic can be sent to any interface, except aggregated SONET/SDH, aggregated Ethernet, loopback (lo0), or administrative (**fxp0**) interfaces. To send port-mirrored traffic to multiple flow servers or packet analyzers, you can use the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level.

Figure 53: Active Flow Monitoring—Multiple Port Mirroring with Next-Hop Groups Topology Diagram

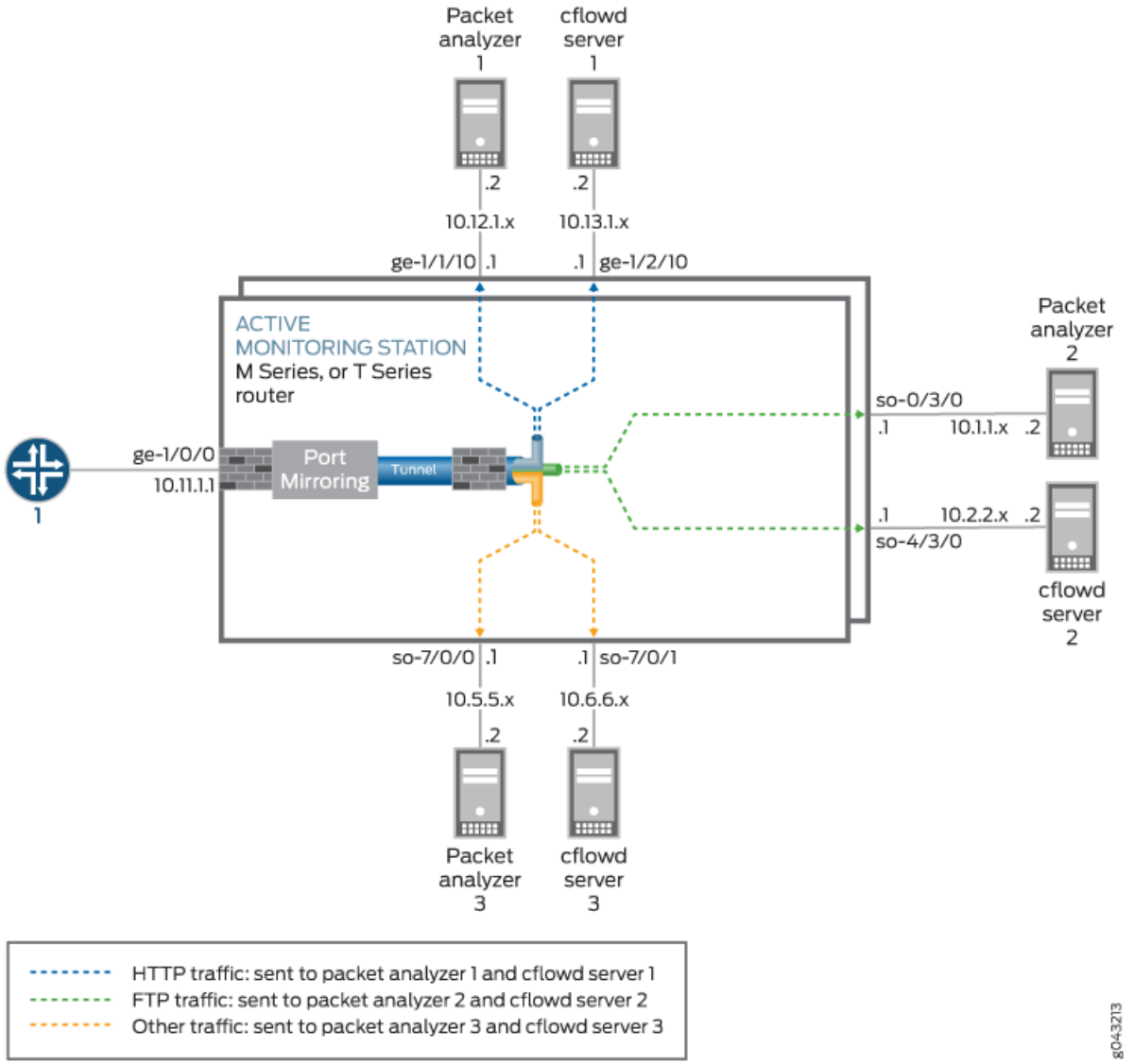


Figure 53 on page 1408 shows an example of how to configure multiple port mirroring with next-hop groups. All traffic enters the monitoring router at interface ge-1/0/0. A firewall filter counts and port-mirrors all incoming packets to a Tunnel Services PIC. A second filter is applied to the tunnel interface and splits the traffic into three categories: HTTP traffic, FTP traffic, and all other traffic. The three types of traffic are assigned to three separate next-hop groups. Each next-hop group contains a unique pair of exit interfaces that lead to different groups of packet analyzers and flow servers.

NOTE: Instances enabled to mirror packets to different destinations from the same PFE, also use different sampling parameters for each instance. When we configure Layer2 Port-mirroring with both global port-mirroring and instance based port-mirroring, PIC level instances will override FPC level and the FPC level will override the Global instance.

```
[edit]
interfaces {
   ge-1/0/0 { # This is the input interface where packets enter the router.
      unit 0 {
         family inet {
            filter {
               input mirror_pkts; # Here is where you apply the first filter.
            }
            address 10.11.1.1/24;
         }
      }
   }
   ge-1/1/0 { # This is an exit interface for HTTP packets.
      unit 0 {
         family inet {
            address 10.12.1.1/24;
         }
      }
   }
   ge-1/2/0 { # This is an exit interface for HTTP packets.
      unit 0 {
         family inet {
            address 10.13.1.1/24;
         }
      }
   }
   so-0/3/0 { # This is an exit interface for FTP packets.
      unit 0 {
         family inet {
            address 10.1.1.1/30;
         }
      }
   }
   so-4/3/0 { # This is an exit interface for FTP packets.
      unit 0 {
         family inet {
```

```
            address 10.2.2.1/30;
          }
        }
    }
    so-7/0/0 { # This is an exit interface for all remaining packets.
        unit 0 {
          family inet {
            address 10.5.5.1/30;
          }
        }
    }
    so-7/0/1 { # This is an exit interface for all remaining packets.
        unit 0 {
          family inet {
            address 10.6.6.1/30;
          }
        }
    }
    vt-3/3/0 { # The tunnel interface is where you send the port-mirrored traffic.
        unit 0 {
          family inet;
        }
        unit 1 {
          family inet {
            filter {
              input collect_pkts;  # This is where you apply the second firewall filter.
            }
          }
        }
    }
}
forwarding-options {
    port-mirroring { # This is required when you configure next-hop groups.
        family inet {
          input {
            rate 1; # This port-mirrors all packets (one copy for every packet received).
          }
          output { # Sends traffic to a tunnel interface to enable multiport mirroring.
            interface vt-3/3/0.1;
            no-filter-check;
          }
        }
    }
    next-hop-group ftp-traffic { # Point-to-point interfaces require you to specify the
```

```
        interface so-4/3/0.0; # interface name.
        interface so-0/3/0.0;
    }
    next-hop-group http-traffic { # Configure a next hop for all multipoint interfaces.
        interface ge-1/1/0.0 {
            next-hop 10.12.1.2;
        }
        interface ge-1/2/0.0 {
            next-hop 10.13.1.2;
        }
    }
    next-hop-group default-collect {
        interface so-7/0/0.0;
        interface so-7/0/1.0;
    }
}
firewall {
    family inet {
        filter mirror_pkts { # Apply this filter to the input interface.
            term catch_all {
                then {
                    count input_mirror_pkts;
                    port-mirror; # This action sends traffic to be copied and port-mirrored.
                }
            }
        }
        filter collect_pkts { # Apply this filter to the tunnel interface.
            term ftp-term { # This term sends FTP traffic to an FTP next-hop group.
                from {
                    protocol ftp;
                }
                then next-hop-group ftp-traffic;
            }
            term http-term { # This term sends HTTP traffic to an HTTP next-hop group.
                from {
                    protocol http;
                }
                then next-hop-group http-traffic;
            }
            term default { # This sends all remaining traffic to a final next-hop group.
                then next-hop-group default-collectors;
            }
        }
    }
```

```
}
```

RELATED DOCUMENTATION

Understanding Port Mirroring

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

Example: Layer 2 Port Mirroring to Multiple Destinations

On MX Series routers, you can mirror traffic to multiple destinations by configuring next-hop groups in Layer 2 port-mirroring firewall filters applied to tunnel interfaces.

1. Configure the chassis to support tunnel services at PIC 0 on FPC 2. This configuration includes two logical tunnel interfaces on FPC 2, PIC 0, port 10.

```
[edit]
chassis {
    fpc 2 {
        pic 0 {
            tunnel-services {
                bandwidth 1g;
            }
        }
    }
}
```

2. Configure the physical and logical interfaces for three bridge domains and one Layer 2 VPN CCC:

   - Bridge domain **bd** will span logical interfaces **ge-2/0/1.0** and **ge-2/0/1.1**.
   - Bridge domain **bd_next_hop_group** will span logical interfaces **ge-2/2/9.0** and **ge-2/0/2.0**.
   - Bridge domain **bd_port_mirror** will use the logical tunnel interface **lt-2/0/10.2**.
   - Layer 2 VPN CCC **if_switch** will connect logical interfaces **ge-2/0/1.2** and **lt-2/0/10.1**.

```
[edit]
interfaces {
    ge-2/0/1 {
        flexible-vlan-tagging;
```

```
    encapsulation flexible-ethernet-services;
    unit 0 { # An interface on bridge domain 'bd'.
      encapsulation vlan-bridge;
      vlan-id 200;
      family bridge {
        filter {
          input pm_bridge;
        }
      }
    }
    unit 1 { # An interface on bridge domain 'bd'.
      encapsulation vlan-bridge;
      vlan-id 201;
      family bridge {
        filter {
          input pm_bridge;
        }
      }
    }
    unit 2 {
      encapsulation vlan-ccc;
      vlan-id 1000;
    }
  }
  ge-2/0/2 { # For 'bd_next_hop_group'
    encapsulation ethernet-bridge;
    unit 0 {
      family bridge;
    }
  }
  lt-2/0/10 {
    unit 1 {
      encapsulation ethernet-ccc;
      peer-unit 2;
    }
    unit 2 {
      encapsulation ethernet-bridge;
      peer-unit 1;
      family bridge {
        filter {
          output redirect_to_nhg;
        }
      }
    }
```

```
    }
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 { # For 'bd_next_hop_group'
            family bridge;
        }
    }
}
```

3. Configure the three bridge domains and the Layer 2 VPN switching CCC:

- Bridge domain **bd** spans logical interfaces **ge-2/0/1.0** and **ge-2/0/1.1**.
- Bridge domain **bd_next_hop_group** spans logical interfaces **ge-2/2/9.0** and **ge-2/0/2.0**.
- Bridge domain **bd_port_mirror** uses the logical tunnel interface **lt-2/0/10.2**.
- Layer 2 VPN CCC **if_switch** connects interfaces **ge-2/0/1.2** and **lt-2/0/10.1**.

```
[edit]
bridge-domains {
    bd {
        interface ge-2/0/1.0;
        interface ge-2/0/1.1;
    }
    bd_next_hop_group {
        interface ge-2/2/9.0;
        interface ge-2/0/2.0;
    }
    bd_port_mirror {
        interface lt-2/0/10.2;
    }
}
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ge-2/0/1.2;
            interface lt-2/0/10.1;
        }
    }
}
```

For detailed information about configuring the CCC connection for Layer 2 switching cross-connects, see the *MPLS Applications User Guide*.

4. Configure forwarding options:

   - Configure global port-mirroring properties to mirror **family vpls** traffic to an interface on the bridge domain **bd_port_mirror**.
   - Configure the next-hop group **nhg_mirror_to_bd** to forward Layer 2 traffic to the bridge domain **bd_next_hop_group**.

   Both of these forwarding options will be referenced by the port-mirroring firewall filter:

```
[edit]
forwarding-options {
    port-mirroring { # Global port mirroring properties.
        input {
            rate 1;
        }
        family vpls {
            output {
                interface lt-2/0/10.2; # Interface on 'bd_port_mirror' bridge domain.
                no-filter-check;
            }
        }
    }
    next-hop-group nhg_mirror_to_bd { # Configure a next-hop group.
        group-type layer-2; # Specify 'layer-2' for Layer 2; default 'inet' is for Layer 3.
        interface ge-2/0/2.0; # Interface on 'bd_next_hop_group' bridge domain.
        interface ge-2/2/9.0; # Interface on 'bd_next_hop_group' bridge domain.
    }
}
```

5. Configure two Layer 2 port-mirroring firewall filters for **family bridge** traffic:

   - **filter_pm_bridge**—Sends all **family bridge** traffic to the global port mirroring destination.
   - **filter_redirect_to_nhg**—Sends all **family bridge** traffic to the final next-hop group **nhg_mirror_to_bd**.

   Layer 2 port-mirroring firewall filters for **family bridge** traffic applies to traffic on a physical interface configured with encapsulation **ethernet-bridge**.

```
[edit]
firewall {
    family bridge {
```

```
        filter filter_pm_bridge {
            term term_port_mirror {
                then port-mirror;
            }
        }
        filter filter_redirect_to_nhg {
            term term_nhg {
                then next-hop-group nhg_mirror_to_bd;
            }
        }
    }
}
```

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | 1200
- Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | 1401
- Defining a Layer 2 Port-Mirroring Firewall Filter | 1343
- Defining a Next-Hop Group for Layer 2 Port Mirroring | 1402
- Displaying Next-Hop Group Settings and Status | 1457

CHAPTER 41

Configuring Port Mirroring for Remote Destinations

IN THIS CHAPTER

- Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN | 1417
- Configuration Layer 2 Port Mirroring to a Remote VLAN | 1418
- Example: Configuring Layer 2 Port Mirroring to Remote VLAN | 1420

Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN

You configure port mirroring on an EX9200 switch to send copies of traffic to an output destination, such as an interface, a routing-instance, or a VLAN; and for the input traffic, you can configure a firewall filter term with various match conditions and actions.

When you configure VLAN as the output destination in a port-mirroring configuration, the traffic for each port-mirroring session is carried over a user-specified VLAN that is dedicated for that mirroring session in all participating switches. The mirrored traffic is copied onto that VLAN (also called as mirror VLAN) and forwarded to interfaces, which are members of the mirror VLAN. The destination interfaces, which are members of the mirror VLAN, can span across multiple switches in the network provided that the same remote mirroring VLAN is used for a mirroring session in all the switches.

You can use the **port-mirror** or **port-mirror-instance** action in the firewall filter configuration when you mirror traffic to remote destinations by configuring a VLAN as a port-mirroring output destination.

RELATED DOCUMENTATION

Understanding Layer 2 Port Mirroring | 1200

Configuration Layer 2 Port Mirroring to a Remote VLAN | 1418

Defining a Layer 2 Port-Mirroring Firewall Filter | 1343

Configuration Layer 2 Port Mirroring to a Remote VLAN

IN THIS SECTION

- Configuring Port Mirroring to a Remote VLAN | 1418

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy the following packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable port mirroring that you have configured when you are not using them.
- Specify individual interfaces as input rather than specifying all interfaces as input in a port mirroring configuration.
- Limit the amount of mirrored traffic by:
  - Using statistical sampling.
  - Setting ratios to select statistical samples.
  - Using firewall filters.

Configuring Port Mirroring to a Remote VLAN

To filter packets to be mirrored to a port-mirroring instance, create the instance and then use it as the action in the firewall filter. You can use firewall filters in both local and remote mirroring configurations.

If the same port-mirroring instance is used in multiple filters or terms, the packets are copied to the port-mirroring output port or port-mirroring VLAN only once.

To filter mirrored traffic, create a port-mirroring instance under the **[edit forwarding-options]** hierarchy level, and then create a firewall filter. The filter can use any of the available match conditions and must

have **port-mirror-instance** *instance-name* as an action. This action in the firewall filter configuration provides the input to the port-mirroring instance.

To configure a port-mirroring instance with firewall filters:

1. Configure the port-mirroring instance name and set the output destination to a VLAN:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance instance-name output vlan (vlan-ID | vlan-name)
   ```

   For example, configure a port-mirroring instance **employee-monitor** and set the output destination to a VLAN ID **999**:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output vlan 999
   ```

2. Create a firewall filter by using any of the available match conditions and assign the port-mirroring instance name as an action in the firewall filter configuration.

   ```
   [edit firewall family ethernet-switching]
   user@switch set filter filter-name term term-name from match-condition
   user@switch set filter filter-name term term-name then match-condition
   user@switch# set filter filter-name term term-namethen port-mirror-instance instance-name
   ```

   For example, create a firewall filter called **example-filter** with two terms **no-analyzer** and **to-analyzer**, and assign the **to-analyzer** term to the **employee-monitor** port-mirroring instance:

   a. Create the first term to define the traffic that should not pass through to the port-mirroring instance **employee-monitor**:

      ```
      [edit firewall family ethernet-switching]
      user@switch# set filter (Firewall Filters) example-filter term no-analyzer from source-address
      192.0.2.14
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term no-analyzer from protocol tcp
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term no-analyzer then accept
      ```

   b. Create the second term to define the traffic that should pass through to the port-mirroring instance **employee-monitor**:

      ```
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term to-analyzer from destination-port 80
      [edit firewall family ethernet-switching]
      ```

```
user@switch# set filter example-filter term to-analyzer then port-mirror-instance
employee–monitor
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then accept
```

3. Apply the firewall filter to an interface or VLAN that provides input to the port-mirroring instance.

   To apply a firewall filter to an interface:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching filer (input | output)
   filter-name
   ```

   To apply a firewall filter to a VLAN:

   ```
   [edit]
   user@switch# set vlan (vlan-ID or vlan-name) filter (input | output) filter-name
   ```

   For example, to apply the **example-filter** firewall filter to the ge-0/0/1 interface:

   ```
   [edit]
   user@switch# set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input example-filter
   ```

   For example, to apply the **example-filter** filter to the **source-vlan** VLAN:

   ```
   [edit]
   user@switch# set vlan source-vlan filter input example-filter
   ```

RELATED DOCUMENTATION

Example: Configuring Layer 2 Port Mirroring to Remote VLAN | 1420

Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN | 1417

Example: Configuring Layer 2 Port Mirroring to Remote VLAN

IN THIS SECTION

- Requirements | 1421
- Overview and Topology | 1422

Mirroring Employee-to-Web Traffic for Remote Analysis | 1422
Verification | 1427

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or existing a VLAN

You can analyze the mirrored traffic by using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN so that you can perform analysis from a remote monitoring station. The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario but includes a filter to mirror only the employee traffic going to the Web.

BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

This example describes how to configure remote mirroring:

Requirements

Before you configure remote mirroring, be sure that:

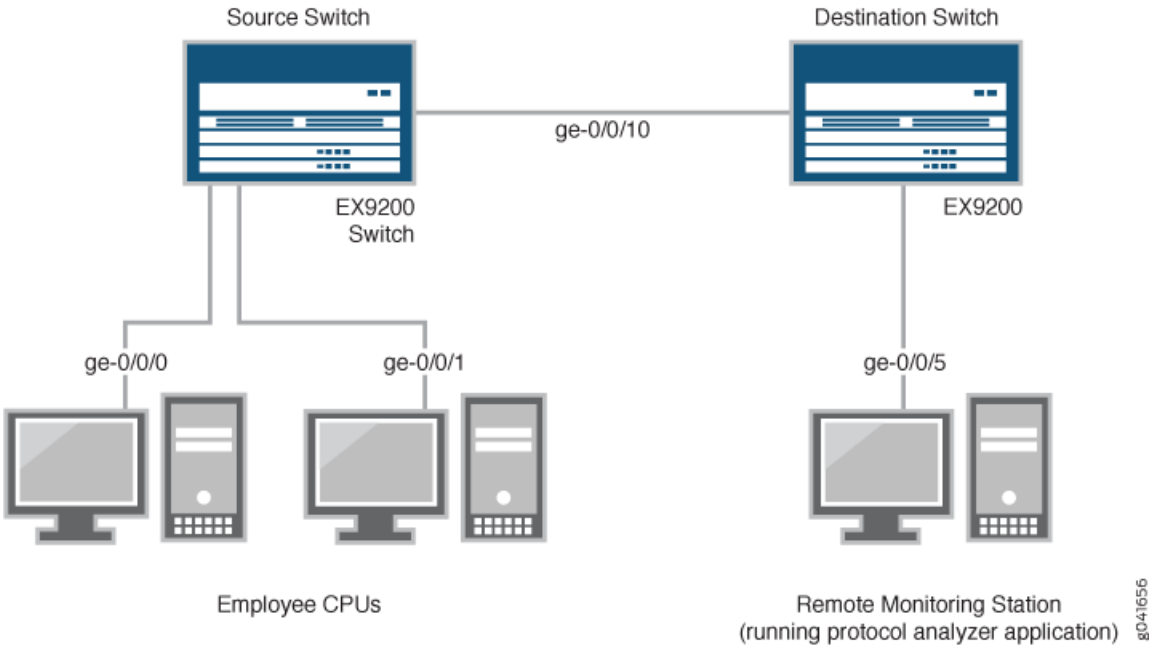
- You have an understanding of mirroring concepts.
- The interfaces that port-mirroring will use as output interfaces have been configured on the switch.

Overview and Topology

This topic includes two related examples that describe how to configure mirroring to the **remote-analyzer** VLAN so that analysis can be performed from a remote monitoring station. The first example shows how to configure a switch to mirror all traffic from employee computers. The second example shows the same scenario, but the setup includes a filter to mirror only the employee traffic going to the Web.

Figure 45 on page 1247 shows the network topology for both these example scenarios.

Figure 54: Remote Mirroring Network Topology Example



In this example:

a. Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 2 interface (both interfaces on the source switch) that serve as connections for employee computers.

b. Interface ge-0/0/10 is a Layer 2 interface that connects the source switch to the destination switch.

c. Interface ge-0/0/5 is a Layer 2 interface that connects the destination switch to the remote monitoring station.

d. VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring Employee-to-Web Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis of employee-to-Web traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port-mirroring to mirror employee traffic to the external Web, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch terminal window:

```
[edit]
set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then
port-mirror-instance employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

- Copy and paste the following commands in the destination switch terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members 999
```

Step-by-Step Procedure

To configure port mirroring of all traffic from the two ports connected to employee computers to the **remote-analyzer** VLAN for use from a remote monitoring station:

1. On the source switch:
   a. Configure the **employee-web-monitor** port-mirroring instance:

```
[edit ]
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode access
```

```
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output
vlan 999
```

b. Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

c. Configure the interface to associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

d. Configure the firewall filter called **watch-employee**:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

In this configuration, the **employee-to-corp** term defines that traffic from destination-address **192.0.2.16/28** and source address **192.0.2.16/28** can be accepted to pass through the switch, and the **employee-to-web** term defines that traffic from port **80** must be sent to the port-mirroring instance **employee-web-monitor**.

e. Apply the firewall filter to the employee interfaces:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

2. On the destination switch:

- Configure the VLAN ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the interface on the destination switch for access mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the interface connected to the destination switch for access mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/5 unit 0 family ethernet-switching vlan members 999
```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
```

```
        }
    }
}
firewall {
    family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
                from {
                    source-address {
                        192.0.2.16/28;
                    }
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then accept;
            }
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
    }
}
forwarding-options {
    analyzer employee-web-monitor {
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch> show
```

```
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying That the Port-Mirroring Instance Has Been Correctly Created | **1427**

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Port-Mirroring Instance Has Been Correctly Created

Purpose

Verify that the port-mirror instance **employee-web-monitor** has been created on the switch with the appropriate output VLAN.

Action

You can verify that the port-mirror is configured as expected by using the **show forwarding-options port-mirror** command. To view previously created analyzers that are disabled, go to the J-Web interface.

To verify that the port-mirror is configured as expected while monitoring employee traffic on the source switch, run the **show forwarding-options port-miror** command on the source switch. The following output is displayed for this configuration example:

```
user@switch> show forwarding-options port-mirror
```

```
Instance Name: employee-web-monitor
  Instance Id: 3
  Input parameters:
    Rate                 : 1
    Run-length           : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination                    Next-hop
    ethernet-switching  up       default-switch/remote-analyzer
```

Meaning

This output shows that the **employee-web-monitor** instance has a ratio of 1 (mirroring every packet, which is the default), the maximum size of the original packet that was mirrored (0 indicates the entire packet), the state of the configuration is up (which indicates the proper state and that the analyzer is programmed, is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and is sending the mirrored traffic to the VLAN called **remote-analyzer**).

RELATED DOCUMENTATION

Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN | **1417**

CHAPTER 42

Configuring Port Mirroring Local and Remote Analysis

IN THIS CHAPTER

- Configuring Port Mirroring | 1429
- Configuring Port Mirroring on SRX Devices | 1433
- Examples: Configuring Port Mirroring for Local Analysis | 1436
- Example: Configuring Port Mirroring for Local Analysis | 1444
- Example: Configuring Port Mirroring for Remote Analysis | 1450

Configuring Port Mirroring

IN THIS SECTION

- Configuring Port Mirroring for Local Analysis | 1430
- Configuring Port Mirroring for Remote Analysis | 1431
- Filtering the Traffic Entering an Analyzer | 1432

You use port mirroring to copy packets and send the copies to a device running an application such as a network analyzer or intrusion detection application so that you can analyze traffic without delaying it. You can mirror traffic entering or exiting a port or entering a VLAN, and you can send the copies to a local access interface or to a VLAN through a trunk interface.

We recommend that you disable port mirroring when you are not using it. To avoid creating a performance issue If you do enable port mirroring, we recommend that you select specific input interfaces instead of using the **all** keyword. You can also limit the amount of mirrored traffic by using a firewall filter.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring Port Mirroring*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

NOTE: If you want to create additional analyzers without deleting an existing analyzer, first disable the existing analyzer by using the **disable analyzer *analyzer-name*** command.

NOTE: You must configure port mirroring output interfaces as **family ethernet-switching**.

Configuring Port Mirroring for Local Analysis

To mirror interface traffic to a local interface on the switch:

1. If you want to mirror traffic that is ingressing or egressing specific interfaces, choose a name for the port-mirroring configuration and configure what traffic should be mirrored by specifying the interfaces and direction of traffic:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input (ingress | egress) interface interface-name
   ```

   NOTE: If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs. If you do so, some VLAN packets might contain incorrect VLAN IDs.

   NOTE: If you configure mirroring for packets that egress an access interface, the original packets lose any VLAN tags when they exit the access interface, but the mirrored (copied) packets retain the VLAN tags when they are sent to the analyzer system.

2. If you want to specify that all traffic entering a VLAN should be mirrored, choose a name for the port-mirroring configuration and specify the VLAN:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input ingress vlan vlan-name
   ```

NOTE: You cannot configure port mirroring to copy traffic that egresses a VLAN.

3. Configure the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

Configuring Port Mirroring for Remote Analysis

To mirror traffic to a VLAN for analysis at a remote location:

1. Configure a VLAN to carry the mirrored traffic:

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

2. Configure the interface that connects to another switch (the uplink interface) to trunk mode and associate it with the appropriate VLAN:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching port-mode trunk vlan members (vlan-name | vlan-id)
```

3. Configure the analyzer:
   a. Choose a name for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name
```

   b. Specify the interface to be mirrored and whether the traffic should be mirrored on ingress or egress:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input (ingress | egress) interface interface-name
```

   c. Specify the appropriate IP address or VLAN as the output (a VLAN is specified in this example:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan (vlan-name | vlan-id)
```

   If you specify an IP address as the output, note the following constraints:

   - The address cannot be in the same subnetwork as any of the switch management interfaces.

- If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (**inet.0** routing table).
- The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.)

Filtering the Traffic Entering an Analyzer

> **NOTE:** This functionality is not supported on NFX150 devices.

In addition to specifying which traffic to mirror by configuring an analyzer, you can also use a firewall filter to exercise more control over which packets are copied. For example, you might use a filter to specify that only traffic from certain applications be mirrored. The filter can use any of the available match conditions and must have an action of modifier of **port-mirror-instance *instance-name*.** If you use the same analyzer in multiple filters or terms, the output packets are copied only once.

When you use a firewall filter as the input to a port-mirroring instance, you send the copied traffic to a local interface or a VLAN just as you do when a firewall is not involved.

To configure port mirroring with filters:

1. Configure a port-mirroring instance for local or remote analysis. Configure only the output. For example, for local analysis enter:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring-instance instance-name output interface interface-name
   ```

   > **NOTE:** You cannot configure input to this instance.

2. Create a firewall filter using any of the available match conditions. In a **then** term, specify include the action modifier **port-mirror-instance *instance-name***.

3. Apply the firewall filter to the interfaces or VLAN that should provide the input to the analyzer:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching filter input filter-name
   [edit]
   ```

```
user@switch# set vlan (vlan-name | vlan-id) filter input filter-name
```

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Examples: Configuring Port Mirroring for Local Analysis | 1436

Example: Configuring Port Mirroring for Remote Analysis | 1450

Overview of Firewall Filters (QFX Series)

Configuring Port Mirroring on SRX Devices

To configure port mirroring on an SRX device, you must first configure the **forwarding-options** and **interfaces** at the **[edit]** hierarchy level.

You must configure the **forwarding-options** statement to define an instance of the **mirror-to** port for port mirroring and also configure the interface to be mirrored.

> **NOTE:** The mirrored port and the mirror-to port must be under the same Broadcom chipset in an I/O card.

To configure port mirroring:

1. Specify the **rate** and **run-length** at the **[edit forwarding-options port-mirroring input]** hierarchy level:

   > **NOTE:**
   > - **rate**: Ratio of packets to be sampled (1 out of *N*) (1 through 65535)
   > - **run-length**: Number of samples after initial trigger (0 through 20)

   ```
   [edit]
      forwarding-options
         port-mirroring {
               input {
                  rate number;
                  run-length number;
   ```

```
        }
    }
```

2. To send the copies of the packet to the **mirror-to** port, include the **interface *intf-name*** statement at the **[edit forwarding-options port-mirroring family any output]** hierarchy level.

```
output {
    interface intf-name;
}
```

> **NOTE:** Port mirroring on SRX devices uses **family any** to transfer the **mirror-to** port information to the Packet Forwarding Engine (PFE). The mirroring engine copies all the packets from **mirrored** port to the **mirror-to** port.

NOTE: You can configure an **instance** clause to specify multiple **mirror-to** ports.

To mirror an interface, include the **port-mirror-instance** statement at the **[edit interface mirrored-intf-name]** hierarchy level.

The mirrored interface is configured with an instance name, defined in the **forwarding-options**. The **mirrored** port and the **mirror-to** port are linked through that instance.

```
instance {
   inst-name {
      input {
         rate number;
         run-length number;
      }
      family any {
         output {
            interface intf-name;
         }
      }
   }
}
interfaces
      mirrored-intf-name {
         port-mirror-instance instance-name;
      }
```

NOTE: Port mirroring on SRX devices does not differentiate the traffic direction, but mirrors the ingress and egress samples together.

A sample configuration for port mirroring is shown below:

```
mirror port ge-1/0/2 to port ge-1/0/9.0
forwarding-options
   port-mirroring {
      input {
         rate 1;
         run-length 10;
      }
      family any {
         output {
```

```
            interface ge-1/0/9.0;
          }
        }
        instance {
          inst1 {
            input {
              rate 1;
              run-length 10;
            }
            family any {
              output {
                interface ge-1/0/9.0;
              }
            }
          }
        }
interfaces {
    ge-1/0/2 {
        port-mirror-instance inst1;
    }
}
```

Examples: Configuring Port Mirroring for Local Analysis

IN THIS SECTION

- Requirements | **1437**
- Overview and Topology | **1437**
- Example: Mirroring All Employee Traffic for Local Analysis | **1438**
- Example: Mirroring Employee Web Traffic with a Firewall Filter | **1439**

Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring copies packets entering or exiting an interface or entering a VLAN and sends the copies to a local interface for local monitoring.

NOTE: This example uses the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

This example describes how to configure port mirroring to copy traffic sent by employee computers to a switch to an access interface on the same switch.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2
- A switch

Overview and Topology

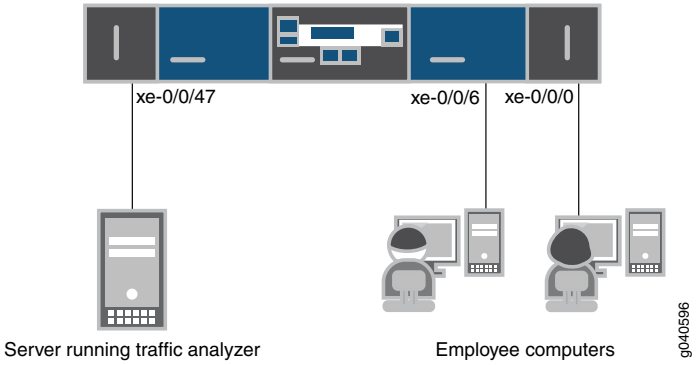
This topic includes two related examples that describe how to mirror traffic entering interfaces on the switch to an access interface on the same switch. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the employee traffic going to the Web.

In this example, **xe-0/0/0** and **xe-0/0/6** serve as connections for employee computers. Interface **xe-0/0/47** is connected to a device running an analyzer application.

NOTE: Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

Figure 52 on page 1352 shows the network topology for this example.

Figure 55: Network Topology for Local Port Mirroring Example



Example: Mirroring All Employee Traffic for Local Analysis

To configure port mirroring for all traffic sent by employee computers for local analysis, perform the tasks explained in this section.

CLI Quick Configuration

To quickly configure local port mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into a switch terminal window:

```
[edit]
set interfaces xe-0/0/0 unit 0 family ethernet-switching
set interfaces xe-0/0/6 unit 0 family ethernet-switching
set interfaces xe-0/0/47 unit 0 family ethernet-switching
set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/6.0
set forwarding-options analyzer employee-monitor output interface xe-0/0/47.0
```

Step-by-Step Procedure

To configure an analyzer called **employee-monitor** and specify the input (source) interfaces and the output interface:

1. Configure the interfaces connected to employee computers as input interfaces for the port-mirror analyzer **employee-monitor**:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/6.0
   ```

2. Configure the output analyzer interface for the **employee-monitor** analyzer. This will be the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface xe-0/0/47.0
   ```

Results

Check the results of the configuration:

```
[edit]
user@switch# show forwarding-options analyzer
   employee-monitor {
      input {
         ingress {
            interface xe-0/0/0.0;
            interface xe-0/0/6.0;
         }
      }
      output {
         interface {
            xe-0/0/47.0;
         }
      }
   }
}
```

Example: Mirroring Employee Web Traffic with a Firewall Filter

IN THIS SECTION

- Requirements | **1439**
- Overview | **1439**
- Configuring | **1440**
- Verification | **1443**

Requirements

This example uses the following hardware and software components:

- One QFX5100 switch
- Junos OS Release 14.1X53-D30

Overview

Rather than mirror all traffic, it is usually desirable to mirror only certain traffic. This is a more efficient use of your bandwidth and hardware and might be necessary due to constraints on these assets. To select specific traffic for mirroring, you use a firewall filter to match the desired traffic and direct it to a port-mirroring instance. The port-mirroring instance then copies the packets and sends them to the output VLAN, interface, or IP address.

Configuring

To specify that the only traffic that will be mirrored is traffic sent by employees to the Web, perform the tasks explained in this section. To select this traffic for mirroring, you use a firewall filter to specify this traffic and direct it to a port-mirroring instance.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set interface xe-0/0/47 unit 0 family ethernet-switching
set forwarding-options port-mirroring instance employee–web–monitor family ethernet-switching output interface xe-0/0/47.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from ip-destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from ip-source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirror-instance employee-web-monitor
set interfaces xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-web traffic from the two ports connected to employee computers:

1. Configure the output interface:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/47 unit 0 family ethernet-switching
   ```

2. Configure the **employee-web-monitor** output interface. (Configure only the output—the input comes from the filter.)

```
[edit forwarding-options]
user@switch# set port-mirroring instance employee–web–monitor family ethernet-switching
output interface xe-0/0/47.0
```

3. Configure a firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the port-mirroring instance **employee-web-monitor**. Traffic to and from the corporate subnet (destination or source address of **192.0.2.16/28**) does not need to be copied, so create another term to accept that traffic before it reaches the term that sends Web traffic to the instance:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from ip-destination-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from ip-source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter (egress filters do not allow analyzers):

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
    port-mirroring {
        instance {
            employee-web-monitor {
                family ethernet-switching {
                    output {
                        interface xe-0/0/47.0;
                    }
                }
            }
```

```
        }
    }
}
...
firewall {
    family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
            from {
                ip-source-address 192.0.2.16/28;
                ip-destination-address 192.0.2.16/28;
            }
            then accept;
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
    }
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
    xe-0/0/47 {
        family ethernet-switching;
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the port-mirroring instance named **employee-web-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify that the port mirror port-mirroring instance has been configured as expected by using the **show forwarding-options port-mirroring** command.

```
user@switch> show forwarding-options port-mirroring
```

```
Instance name                : employee-web-monitor
Instance Id:  2
Input parameters:
 Rate                            :1
 Run-length                      :0
 Maximum packet length           :0
Output parameters:
 Family                State     Destination      Next-hop
 ethernet-switching    up        xe-0/0/47.0
```

Meaning

This output shows the following information about the port-mirroring instance **employee-web-monitor**:

- Has a rate of **1** (mirroring every packet, the default setting)
- The number of consecutive packets sampled (run-length) is **0**
- The maximum size of the original packet that was mirrored is **0** (**0** indicates the entire packet)
- The state of the output parameters: **up** indicates that the instance is mirroring the traffic entering the xe-0/0/0 and xe-0/0/6 interfaces, and is sending the mirrored traffic to the xe-0/0/47 interface

If the state of the output interface is **down** or if the output interface is not configured, the **state** value will be **down** and the instance will not be programmed for mirroring.

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | **1175**

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Configuring Port Mirroring | 1429

Example: Configuring Port Mirroring for Remote Analysis | 1450

Example: Configuring Port Mirroring for Local Analysis

IN THIS SECTION

- Requirements | 1444
- Overview and Topology | 1445
- Mirroring All Employee Traffic for Local Analysis | 1445
- Mirroring Employee-to-Web Traffic for Local Analysis | 1447
- Verification | 1449

Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring copies packets entering or exiting an interface or entering a VLAN and sends the copies to a local interface for local monitoring.

NOTE: This example uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Examples: Configuring Port Mirroring for Local Analysis" on page 1436. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

This example describes how to configure port mirroring to copy traffic sent by employee computers to a switch to an access interface on the same switch.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.1
- A switch

Overview and Topology

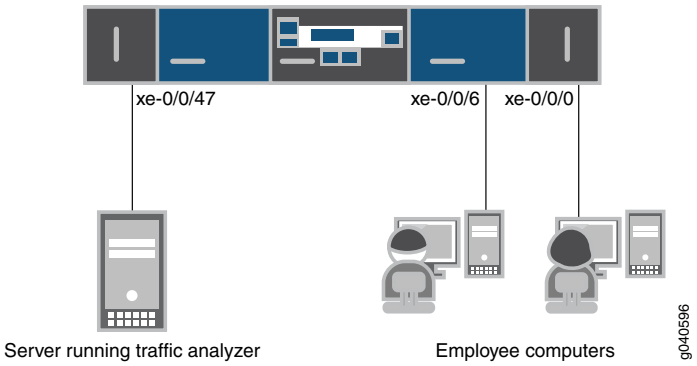
This topic includes two related examples that describe how to mirror traffic entering interfaces on the switch to an access interface on the same switch. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the employee traffic going to the Web.

In this example, **xe-0/0/0** and **xe-0/0/6** serve as connections for employee computers. Interface **xe-0/0/47** is connected to a device running an analyzer application.

> **NOTE:** Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

Figure 52 on page 1352 shows the network topology for this example.

Figure 56: Network Topology for Local Port Mirroring Example



Mirroring All Employee Traffic for Local Analysis

To configure port mirroring for all traffic sent by employee computers for local analysis, perform the tasks explained in this section.

CLI Quick Configuration

To quickly configure local port mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into a switch terminal window:

```
[edit]
```

set interfaces xe-0/0/0 unit 0 family ethernet-switching

set interfaces xe-0/0/6 unit 0 family ethernet-switching

set interfaces xe-0/0/47 unit 0 family ethernet-switching

set ethernet-switching-options analyzer employee-monitor input ingress interface xe-0/0/0.0

set ethernet-switching-options analyzer employee-monitor input ingress interface xe-0/0/6.0

set ethernet-switching-options analyzer employee-monitor output interface xe-0/0/47.0

Step-by-Step Procedure

To configure an analyzer called **employee-monitor** and specify the input (source) interfaces and the output interface:

1. Configure the interfaces connected to employee computers as input interfaces for the port-mirror analyzer **employee-monitor**:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/6.0
   ```

2. Configure the output analyzer interface for the **employee-monitor** analyzer. This will be the destination interface for the mirrored packets:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor output interface xe-0/0/47.0
   ```

Results

Check the results of the configuration:

```
[edit]
user@switch# show ethernet-switching-options
   analyzer employee-monitor {
      input {
         ingress {
            interface xe-0/0/0.0;
            interface xe-0/0/6.0;
         }
      }
      output {
         interface {
            xe-0/0/47.0;
         }
      }
   }
}
```

Mirroring Employee-to-Web Traffic for Local Analysis

To mirror only traffic sent by employees to the Web for local analysis, perform the tasks explained in this section.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set ethernet-switching-options analyzer employee–web–monitor output interface xe-0/0/47.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then analyzer employee-web-monitor
set interfaces xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-web traffic from the two ports connected to employee computers:

1. Configure the output interface:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/47 unit 0 family ethernet-switching
   ```

2. Configure the **employee-web-monitor** analyzer output. (Configure only the output—the input comes from the filter.)

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-web-monitor output interface xe-0/0/47.0
   ```

3. Configure a firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the analyzer **employee-web-monitor**. Traffic to and from the corporate subnet (destination or source address of **192.0.2.16/28**) does not need to be copied, so create another term to accept that traffic before it reaches the term that sends Web traffic to the analyzer:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then analyzer
employee-web-monitor
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter (egress filters do not allow analyzers):

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show ethernet-switching-options
    analyzer employee-web-monitor {
        output {
            interface xe-0/0/47.0;
            }
        }
}
...
firewall family ethernet-switching {
    filter watch-employee {
        term employee-to-web {
            from {
                destination-port 80;
            }
            then analyzer employee-web-monitor;
        }
    }
```

```
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** or **employee-web-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify that the port mirror analyzer has been configured as expected using the **show analyzer** command.

`user@switch>` **show analyzer**

```
Analyzer name                : employee-monitor
Output interface             : xe-0/0/47.0
Mirror ratio                 : 1
Loss priority                : Low
Ingress monitored interfaces : xe-0/0/0.0
Ingress monitored interfaces : xe-0/0/6.0
```

```
Egress monitored interfaces  : None
```

Meaning

This output shows that the **employee-monitor** analyzer:

- Has a ratio of 1 (mirroring every packet, the default setting)
- Has a loss priority of low (set this option to high only when the analyzer output is to a VLAN)
- Is mirroring the traffic entering the **xe-0/0/0** and **xe-0/0/6** interfaces
- Is sending the mirrored traffic to the **xe-0/0/47** interface

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Configuring Port Mirroring

Example: Configuring Port Mirroring for Remote Analysis

IN THIS SECTION

- Requirements | 1451
- Overview and Topology | 1451
- Mirroring All Employee Traffic for Remote Analysis | 1451
- Mirroring Employee-to-Web Traffic for Remote Analysis | 1453
- Verification | 1456

Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring copies packets entering or exiting an interface or entering a VLAN and sends the copies either to a local interface for local monitoring or to a VLAN for remote monitoring. This example describes how to configure port mirroring for remote analysis.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2 for the QFX Series
- A switch

Overview and Topology

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to an analyzer VLAN so that you can perform analysis using a remote device. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the employee traffic going to the Web.

In this example:

- Interfaces **ge-0/0/0** and **ge-0/0/1** are Layer 2 interfaces that connect to employee computers.
- Interface **ge-0/0/2** is a Layer 2 interface that connects to another switch.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

> **NOTE:** In addition to performing the configuration steps described here, you must also configure the analyzer VLAN (**remote-analyzer** in this example) on the other switches that are used to connect the source switch (the one in this configuration) to the one that the monitoring station is connected to.

Mirroring All Employee Traffic for Remote Analysis

CLI Quick Configuration

To quickly configure this section of the 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:

```
[edit]
```

set vlans remote-analyzer vlan-id 999

set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999

set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0

set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0

set forwarding-options analyzer employee-monitor output vlan remote-analyzer

Step-by-Step Procedure

To configure basic remote port mirroring:

1. Configure the analyzer VLAN (called **remote-analyzer** in this example):

   ```
   [edit vlans]
   user@switch# set vlans remote-analyzer vlan-id 999
   ```

2. Configure the interface connected to another switch for trunk mode and associate it with the **remote-analyzer** VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
   user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
   ```

3. Configure the **employee-monitor** analyzer:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee–monitor
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
   user@switch# set analyzer employee-monitor output vlan remote-analyzer
   ```

4. Configure the **remote-analyzer** VLAN on the switches that connect this switch to the monitoring workstation.

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
```

```
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
```

Mirroring Employee-to-Web Traffic for Remote Analysis

CLI Quick Configuration

To quickly configure this section of the 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:

```
[edit]
```

set vlans remote-analyzer vlan-id 999

set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk

set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999set forwarding-options port-mirroring instance employee-web-monitor loss-priority high output vlan 999

set firewall family ethernet-switching filter watch-employee term employee-to-web from destination-port 80

set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirror-instance employee-web-monitor employee-web-monitor

set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee

set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee

Step-by-Step Procedure

1. Configure the analyzer VLAN (called **remote-analyzer** in this example):

   ```
   [edit vlans]
   user@switch# set remote-analyzer vlan-id 999
   ```

2. Configure an interface to associate it with the **remote-analyzer** VLAN:

   ```
   [edit interfaces]
   user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
   ```

```
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

3. Configure the **employee-web-monitor** analyzer. (Configure only the output—the input comes from the filter.)

```
[edit forwarding-options]
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
```

4. Configure a firewall filter called **watch-employee** to match traffic sent to the Web and send it to the analyzer **employee-web-monitor**:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance employee-web-monitor
```

5. Apply the firewall filter to the appropriate interfaces as an ingress filter:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filterinput watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

6. Configure the **remote-analyzer** VLAN on the switches that connect this switch to the monitoring workstation.

Results

Check the results of the configuration:

```
[edit]
user@switch# show
interfaces {
    ...
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
```

```
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
}
...
firewall {
    family ethernet-switching {
        ...
        filter watch-employee {
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
    }
}
forwarding-options analyzer {
    employee-web-monitor {
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
```

```
    }
  }
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose

Verify that the analyzer named **employee-monitor** or **employee-web-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action

You can verify the port mirror analyzer is configured as expected using the **show analyzer** command.

`user@switch>` **show analyzer**

```
Analyzer name                : employee-monitor
Output VLAN                  : remote-analyzer
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
```

Meaning

This output shows that the **employee-monitor** analyzer is mirroring the traffic entering **ge-0/0/0** and **ge-0/0/1** and is sending the mirror traffic to the analyzer **remote-analyzer**.

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | **1175**

Configuring Port Mirroring | **1429**

Examples: Configuring Port Mirroring for Local Analysis | **1436**

Overview of Firewall Filters (QFX Series)

CHAPTER 43

Monitoring Port Mirroring

IN THIS CHAPTER

- Displaying Layer 2 Port-Mirroring Instance Settings and Status | 1457
- Displaying Next-Hop Group Settings and Status | 1457

Displaying Layer 2 Port-Mirroring Instance Settings and Status

To display the current state of port-mirroring instances, use the **show forwarding-options port-mirroring <terse | detail> <*instance-name*>** operational command.

For more information about displaying port mirroring instance settings and status, see the *Junos OS Administration Library*.

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | 1200
- Layer 2 Port Mirroring Global Instance | 1308
- *Layer 2 Port Mirroring Named Instances*
- *Configuring the Global Instance of Layer 2 Port Mirroring*
- *Defining a Named Instance of Layer 2 Port Mirroring*
- Disabling Layer 2 Port Mirroring Instances | 1319
- Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis | 1328
- *Example: Layer 2 Port Mirroring with Multiple Instances*

Displaying Next-Hop Group Settings and Status

To display the current state of next-hop groups, use the **show forwarding-options next-hop-group <terse | brief | detail> <*group-name*>** operational command.

For more information, see the CLI Explorer.

RELATED DOCUMENTATION

- Understanding Layer 2 Port Mirroring | **1200**
- Understanding Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups | **1401**
- Defining a Layer 2 Port-Mirroring Firewall Filter | **1343**
- Defining a Next-Hop Group for Layer 2 Port Mirroring | **1402**
- Example: Layer 2 Port Mirroring to Multiple Destinations | **1412**

CHAPTER 44

Troubleshooting Port Mirroring

IN THIS CHAPTER

- Troubleshooting Port Mirroring | 1459
- Troubleshooting Port Mirroring Configuration Error Messages | 1464

Troubleshooting Port Mirroring

IN THIS SECTION

- Port Mirroring Constraints and Limitations | 1459
- Egress Port Mirroring with VLAN Translation | 1463
- Egress Port Mirroring with Private VLANs | 1463

Port Mirroring Constraints and Limitations

IN THIS SECTION

- Local and Remote Port Mirroring | 1459
- Remote Port Mirroring Only | 1461
- Port Mirroring on OCX Series Switches | 1462

Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.

- Each Node group in a QFabric system is subject to the following constraints:
  - Up to four of the configurations can be used for local port mirroring.
  - Up to three of the configurations can be used for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group:
  - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
  - There can be no more than two configurations that mirror egress traffic.
  - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- Configure mirroring in an analyzer (with **set forwarding-options analyzer**) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.
- If you mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are not sent to the output port or VLAN.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.

- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies will have incorrect VLAN IDs.

  This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the same Node device. In this case the mirrored copies will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5xxx (including QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210) and EX4600 (including EX4600 and EX4650) switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.
- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.
- Egress VLAN mirroring is not supported.

Remote Port Mirroring Only

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, that address cannot be in the same subnetwork as any of the switch management interfaces.
- If you create virtual routing instances and you create an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.
- If the output VLAN has more than one member interface, then traffic is mirrored only to the first member of the VLAN, and other members of the same VLAN do not carry any mirrored traffic.

- If you attempt to configure more than one analyzer session for remote port mirroring to an IP address (GRE encapsulation) and the IP addresses of the analyzers are reachable through the same interface, then only one analyzer session is configured.
- The number of possible output interfaces in remote port mirroring varies among the switches in the QFX5K line:
  - QFX5110, QFX5120, QFX5210—Support a maximum of 4 output interfaces
  - QFX5100 and QFX5200—Support a maximum of 3 output interfaces.
- Whenever any member in a remote port mirroring VLAN is removed from that VLAN, reconfigure the analyzer session for that VLAN.

Port Mirroring on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. There can be no more than two configurations that mirror ingress or egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces by using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

RELATED DOCUMENTATION

Understanding Port Mirroring | 1183

Example: Mirroring Employee Web Traffic with a Firewall Filter | 1351

Configuring Port Mirroring

Egress Port Mirroring with VLAN Translation

Problem

Description: If you create a port-mirroring configuration that mirrors customer VLAN (CVLAN) traffic on egress and the traffic undergoes VLAN translation before being mirrored, the VLAN translation does not apply to the mirrored packets. That is, the mirrored packets retain the service VLAN (SVLAN) tag that should be replaced by the CVLAN tag on egress. The original packets are unaffected—on these packets VLAN translation works properly, and the SVLAN tag is replaced with the CVLAN tag on egress.

Solution

This is expected behavior.

SEE ALSO

Understanding Q-in-Q Tunneling and VLAN Translation

Egress Port Mirroring with Private VLANs

Problem

Description: If you create a port-mirroring configuration that mirrors private VLAN (PVLAN) traffic on egress, the mirrored traffic (the traffic that is sent to the analyzer system) has the VLAN tag of the ingress VLAN instead of the egress VLAN. For example, assume the following PVLAN configuration:

- Promiscuous trunk port that carries primary VLANs pvlan100 and pvlan400.
- Isolated access port that carries secondary VLAN isolated200. This VLAN is a member of primary VLAN pvlan100.
- Community port that carries secondary VLAN comm300. This VLAN is also a member of primary VLAN pvlan100.
- Output interface (monitor interface) that connects to the analyzer system. This interface forwards the mirrored traffic to the analyzer.

If a packet for pvlan100 enters on the promiscuous trunk port and exits on the isolated access port, the original packet is untagged on egress because it is exiting on an access port. However, the mirror copy retains the tag for pvlan100 when it is sent to the analyzer.

Here is another example: If a packet for comm300 ingresses on the community port and egresses on the promiscuous trunk port, the original packet carries the tag for pvlan100 on egress, as expected. However, the mirrored copy retains the tag for comm300 when it is sent to the analyzer.

Solution

This is expected behavior.

RELATED DOCUMENTATION

- Understanding Port Mirroring and Analyzers | 1175
- Examples: Configuring Port Mirroring for Local Analysis | 1436
- Example: Configuring Port Mirroring for Remote Analysis | 1450
- Example: Mirroring Employee Web Traffic with a Firewall Filter | 1439

Troubleshooting Port Mirroring Configuration Error Messages

Troubleshooting issues with port mirroring on EX Series switches:

1. An Analyzer Configuration Returns a “Multiple interfaces cannot be configured as a member of Analyzer output VLAN” Error Message | 1464

An Analyzer Configuration Returns a “Multiple interfaces cannot be configured as a member of Analyzer output VLAN” Error Message

Problem

Description: In an analyzer configuration, if the VLAN to which mirrored traffic is sent contains more than one member interface, the following error message is displayed in the CLI when you commit the analyzer configuration and the commit fails:

```
Multiple interfaces cannot be configured as a member of Analyzer output VLAN <vlan
 name>
```

Solution

You must direct the mirrored traffic to a VLAN that has a single member interface. You can do this by completing either of these tasks:

- Reconfigure the existing VLAN to contain a single member interface. You can choose this method if you want to use the existing VLAN.

- Create a new VLAN with a single member interface and associate the VLAN with the analyzer.

To reconfigure the existing VLAN to contain only one member interface:

1. Remove member interfaces from the VLAN repeatedly by using either the **delete vlan** command or the **delete interface** command until the VLAN contains a single member interface:

   - ```
     [edit]
     user@switch#  delete vlan vlan-id interface interface-name
     ```

   - ```
     [edit]
     user@switch#  delete interface interface-name unit 0 family family-name vlan member vlan-id
     ```

2. (Optional) Confirm that the VLAN contains only one interface:

   ```
   [edit]
   user@switch#  show vlans vlan-name
   ```

   The output for this command must display only one interface.

To create a new VLAN with a single member interface:

1. Configure a VLAN to carry the mirrored traffic:

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

2. Associate an interface with the VLAN:

   ```
   [edit]
   user@switch#  set interfaces interface-name unit logical-unit-number family family-name vlan members
   vlan-name
   ```

3. Associate the VLAN with the analyzer:

   ```
   [edit ethernet-switching-options]
   user@switch#  set analyzer analyzer-name output vlan vlan-name
   ```

PART 11

System Log Messages

Overview to System Logging | **1467**

Configuring System Logging for a Single-Chassis System | **1480**

Configuring System Logging for a TX Matrix or TX Matrix Plus Router | **1506**

Directing System Log Messages to a Remote Destination | **1527**

Displaying System Log Files | **1544**

Displaying and Interpreting System Log Message Descriptions | **1548**

Configuring System Logging for a Security Device | **1563**

Monitoring Log Messages | **1591**

CHAPTER 45

Overview to System Logging

IN THIS CHAPTER

- Junos OS System Log Overview | 1467
- Overview of Junos OS System Log Messages | 1468
- Junos OS System Log Configuration Hierarchy | 1469
- Junos OS System Logging Facilities and Message Severity Levels | 1470
- Junos OS Default System Log Settings | 1472
- Junos OS Platform-Specific Default System Log Messages | 1473
- Interpreting Messages Generated in Standard Format | 1475
- Managing Host OS System Log and Core Files | 1476

Junos OS System Log Overview

Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the device, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login to the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred.

In Junos OS Release 17.3R1, the syslog-event daemon is able to handle the fxp0 in dedicated management routing instance for for IPv4 addressed remote host. As of Junos OS Release 18.1R1, the syslog-event daemon supports IPv6-based configuration when connecting to a remote host or an archival site and fxp0 is moved to dedicated management instance. In Junos OS Release 18.4R1, the syslog client can send messages through any routing instance you define at appropriate hierarchies. See **routing-instance (Syslog)**.

NOTE: This topic describes system log messages for Junos OS processes and libraries and not the system logging services on a Physical Interface Card (PIC) such as the Adaptive Services PIC.

RELATED DOCUMENTATION

Junos OS System Log Configuration Hierarchy | 1469

Junos OS Minimum System Logging Configuration | 1486

Overview of Junos OS System Log Messages

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the switch, including the following:

- Routine operations, such as a user login into the configuration database.
- Failure and error conditions, such as failure to access a configuration file.
- Emergency or critical conditions, such as power-down of the switch due to excessive temperature.

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the System Log Explorer.

NOTE: OCX Series switches comprise both the Junos OS and the host operating system (OS). For information about system logging on the host OS, see "Managing Host OS System Log and Core Files" on page 1476.

RELATED DOCUMENTATION

Junos OS System Log Configuration Statements | 1485

Junos OS Minimum System Logging Configuration | 1486

Junos OS System Log Configuration Hierarchy

To configure the router to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string
        match "regular-expression";
        source-address source-address;
        structured-data {
            brief;
        }
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

RELATED DOCUMENTATION

Junos OS System Logging Facilities and Message Severity Levels

Table 147 on page 1470 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 147: Junos OS System Logging Facilities

Facility (number)	Type of Event or Error
kernel (0)	Actions performed or errors encountered by the Junos OS kernel
user (1)	Actions performed or errors encountered by user-space processes
daemon (3)	Actions performed or errors encountered by system processes
authorization (4)	Authentication and authorization attempts
ftp (11)	Actions performed or errors encountered by the FTP process
ntp (12)	Actions performed or errors encountered by the Network Time Protocol processes.
security (13)	Security related events or errors.
dfc (17)	Events related to dynamic flow capture
external (18)	Actions performed or errors encountered by the local external applications.
firewall (19)	Packet filtering actions performed by a firewall filter
pfe (20)	Actions performed or errors encountered by the Packet Forwarding Engine
conflict-log (21)	Specified configuration is invalid on the router type
change-log (22)	Changes to the Junos OS configuration
interactive-commands (23)	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client

Table 148 on page 1471 lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see "Disabling the System Logging of a Facility" on page 1501.

Table 148: System Log Message Severity Levels

Value	Severity Level	Description
N/A	**none**	Disables logging of the associated facility to a destination
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring
5	**notice**	Conditions that are not errors but might warrant special handling
6	**info**	Events or nonerror conditions of interest
7	**any**	Includes all severity levels

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | **1480**

Examples: Configuring System Logging | **1502**

Junos OS Default System Log Settings

Table 149 on page 1472 summarizes the default system log settings that apply to all routers that run the Junos OS, and specifies which statement to include in the configuration to override the default value.

Table 149: Default System Logging Settings

Setting	Default	Overriding Statement	Instructions

Alternative facility for message forwarded to a remote machine	For **change-log**: **local6**
	For **conflict-log**: **local5**
	For **dfc**: **local1**
	For **firewall**: **local3**
	For **interactive-commands**: **local7**
	For **pfe**: **local4**
		[edit system syslog]
		host *hostname* {
		facility-override *facility*;
		}
			"Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 1536

Format of messages logged to a file	Standard Junos OS format, based on UNIX format	[edit system syslog]
		file *filename* {
		structured-data;
		}
			"Logging Messages in Structured-Data Format" on page 1489

Maximum number of files in the archived set	10	[edit system syslog]
		archive {
		files *number*;
		}
		file *filename* {
		archive {
		files *number*;
		}
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 1490

Maximum size of the log file	M Series, MX Series, and T Series: 1 megabyte (MB)
	TX Matrix: 10 MB
		[edit system syslog]
		archive {
		size *size*;
		}
		file *filename* {
		archive {
		size *size*;
		}
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 1490

Table 149: Default System Logging Settings *(continued)*

Setting	Default	Overriding Statement	Instructions
Timestamp format	Month, date, hour, minute, second For example: **Aug 21 12:36:30**	[edit system syslog] time-format *format*;	"Including the Year or Millisecond in Timestamps" on page 1496

Users who can read log files	**root** user and users with the Junos OS **maintenance** permission	[edit system syslog]
		archive {
		world-readable;
		}
		file *filename* {
		archive {
		world-readable;
		}
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 1490

- Junos OS System Log Overview on page 1467
- Junos OS Platform-Specific Default System Log Messages on page 1473

Junos OS Platform-Specific Default System Log Messages

The following messages are generated by default on specific routers. To view any of these types of messages, you must configure at least one destination for messages as described in "Junos OS Minimum System Logging Configuration" on page 1486.

- To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

```
[edit system syslog]
(console | file filename | host destination | user username) {
    kernel info;
}
```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards all messages with a severity of **info** and higher to the master Routing Engine on the TX Matrix router. This is equivalent to the following configuration statement included on the TX Matrix router:

```
[edit system syslog]
```

```
host scc-master {
    any info;
}
```

- Starting in Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, likewise on a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 routers, the master Routing Engine on each T1600 or T4000 LCC forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

  NOTE: From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router controls all the T1600 or T4000 routers connected to it in the routing matrix.

```
[edit system syslog]
host sfc0-master {
    any info;
}
```

Release History Table

Release	Description
15.1X49-D10	Starting in Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, likewise on a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 routers, the master Routing Engine on each T1600 or T4000 LCC forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher.

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

Junos OS Default System Log Settings | **1472**

Routing Matrix with a TX Matrix Plus Router Solutions Page

Interpreting Messages Generated in Standard Format

The syntax of a standard-format message generated by a Junos OS process or subroutine library depends on whether it includes priority information:

- When the **explicit-priority** statement is included at the [*filename*] or [*hostname*] hierarchy level, a system log message has the following syntax:

```
timestamp  message-source: %facility-severity-TAG: message-text
```

- When directed to the console or to users, or when the **explicit-priority** statement is not included for files or remote hosts, a system log message has the following syntax:

```
timestamp  message-source: TAG: message-text
```

Table 150 on page 1475 describes the message fields.

Table 150: Fields in Standard-Format Messages

Field	Description
timestamp	Time at which the message was logged.
message-source	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields: hostname, process and process ID (PID). If the process does not report its PID, the PID is not displayed. The message source subfields are displayed in the following format: `hostname process[process-ID]`
facility	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: Facility Codes Reported in Priority Information in "Including Priority Information in System Log Messages" on page 1492.
severity	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table: Numerical Codes for Severity Levels Reported in Priority Information in "Including Priority Information in System Log Messages" on page 1492.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix. Not all processes on a routing platform use tags, so this field does not always appear.

Table 150: Fields in Standard-Format Messages *(continued)*

Field	Description
message-text	Text of the message.

Managing Host OS System Log and Core Files

IN THIS SECTION

- Viewing Log Files On the Host OS System | **1477**
- Copying Log Files From the Host System To the Switch | **1477**
- Viewing Core Files On the Host OS System | **1477**
- Copying Core Files From the Host System To the Switch | **1478**
- Cleaning Up Temporary Files on the Host OS | **1478**

On Junos OS switches with a host OS, the Junos OS might generates system log messages (also called *syslog messages*) to record events that occur on the switch, including the following:

- Routine operations, such as a user login into the configuration database.
- Failure and error conditions.
- Emergency or critical conditions, such as power-down of the switch due to excessive temperature.

On OCX Series switches:

- System log messages are logged in the **/var/log/dcpfe.log** file in the host OS in the following scenarios:
  - When the forwarding daemon is initialized.
  - Messages are tagged as emergency (LOG_EMERG). A copy of the message is also sent to the **/var/log** directory on the switch.
- Messages from processes are available on the host system in the **/var/log** directory. System log messages from the host chassis management process are recorded in the **lcmd.log** file in the **/var/log** directory.

On QFX switches with a host OS:

- The Junos OS and host OS record log messages for system and process events, and generate core files upon certain system failures.

- These files are stored in directories such as /var/log for log messages, and /var/tmp or /var/crash for core files, depending on the type of host OS running on the switch.

For diagnostic purposes, you can access these host OS system log and core files from the Junos OS CLI on the switch. You can also clean up directories where the host OS stores temporary log and other files.

This topic includes these sections:

Viewing Log Files On the Host OS System

To view a list of the log files created on the host OS, enter the following command:

```
user@switch> show app-engine logs
```

Copying Log Files From the Host System To the Switch

To copy log files from the host OS to the switch, enter the following command:

```
user@switch> request app-engine file-copy log from-jhost source to-vjunos destination
```

For example, to copy the *lcmd* log file to the switch, enter the following command:

```
user@switch> request app-engine file-copy log from-jhost lcmd.log to-vjunos /var/tmp
```

Viewing Core Files On the Host OS System

To view the list of core files generated and stored on the host OS system, enter the following command:

```
user@switch> show app-engine crash
```

The list might look like this example output:

```
Compute cluster: default-cluster
  Compute node: default-node

     Crash Info
     ==========
     total 13480
     -rw-r--r-- 1 root root  178046 Feb 14 23:08
localhost.lcmd.26653.1455520135.core.tgz
     -rw-r--r-- 1 root root 4330343 Feb 15 00:45
```

```
localhost.dcpfe.7155.1455525926.core.tgz
     -rw-r--r-- 1 root root 4285901 Feb 15 01:49
localhost.dcpfe.25876.1455529782.core.tgz
     -rw-r--r-- 1 root root 4288508 Feb 15 02:39
localhost.dcpfe.713.1455532774.core.tgz
     -rw-r--r-- 1 root root  264079 Feb 15 17:02
localhost.lcmd.1144.1455584540.core.tgz
```

Copying Core Files From the Host System To the Switch

To copy core files from the host OS to the switch, enter the following command:

```
user@switch> request app-engine file-copy crash from-jhost source to-vjunos destination-dir-or-file-path
```

When the destination Junos OS path is a directory, the source filename is used by default. To rename the file at the destination, enter the destination argument as a full path including the desired filename.

For example, to copy the *localhost.lcmd.26653.1455520135.core.tgz* core archive file to the switch, enter the following command:

```
user@switch> request app-engine file-copy crash from-jhost localhost.lcmd.26653.1455520135.core.tgz
  to-vjunos /var/tmp
```

To see the results on the switch, enter the following command:

```
user@switch> show system core-dumps
re0:
--------------------------------------------------------------------------
-rw-r--r--  1 root  field     178046 Feb 15 17:15
/var/tmp/localhost.lcmd.26653.1455520135.core.tgz
total files: 1
```

Cleaning Up Temporary Files on the Host OS

To remove temporary files created on the host OS, enter the following command:

```
user@switch> request app-engine cleanup
```

For example, the following sample output on a switch with a Linux host OS shows cleanup of temporary files stored in /var/tmp:

```
Compute cluster: default-cluster

  Compute node: default-node

   Cleanup (/var/tmp)
   =======
```

RELATED DOCUMENTATION

Overview of Junos OS System Log Messages | 1468

CHAPTER 46

Configuring System Logging for a Single-Chassis System

IN THIS CHAPTER

- Single-Chassis System Logging Configuration Overview | 1480
- Overview of Single-Chassis System Logging Configuration | 1482
- Junos OS System Log Configuration Hierarchy | 1484
- Junos OS System Log Configuration Statements | 1485
- Junos OS Minimum System Logging Configuration | 1486
- Example: Configuring System Log Messages | 1487
- Logging Messages in Structured-Data Format | 1489
- Specifying Log File Size, Number, and Archiving Properties | 1490
- Including Priority Information in System Log Messages | 1492
- System Log Facility Codes and Numerical Codes Reported in Priority Information | 1494
- Including the Year or Millisecond in Timestamps | 1496
- Using Strings and Regular Expressions to Refine the Set of Logged Messages | 1497
- Junos System Log Regular Expression Operators for the match Statement | 1500
- Disabling the System Logging of a Facility | 1501
- Examples: Configuring System Logging | 1502
- Examples: Assigning an Alternative Facility | 1504

Single-Chassis System Logging Configuration Overview

The Junos system logging utility is similar to the UNIX **syslogd** utility. This section describes how to configure system logging for a single-chassis system that runs the Junos OS.

System logging configuration for the Junos-FIPS software and for Juniper Networks routers in a Common Criteria environment is the same as for the Junos OS. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

For information about configuring system logging for a routing matrix composed of a TX Matrix router and T640 routers, see "Configuring System Logging for a TX Matrix Router" on page 1506.

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions. You always specify the facility and severity of the messages to include in the log. For more information, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

You direct messages to one or more destinations by including the appropriate statement at the **[edit system syslog]** hierarchy level:

- To a named file in a local file system, by including the **file** statement. See "Directing System Log Messages to a Log File" on page 1530.
- To the terminal session of one or more specific users (or all users) when they are logged in to the router, by including the **user** statement. See "Directing System Log Messages to a User Terminal" on page 1531.
- To the router console, by including the **console** statement. See "Directing System Log Messages to the Console" on page 1531.
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine on the router, by including the **host** statement.

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the System Log Explorer. You can alter the content and format of logged messages in the following ways:

- You can log messages to a file in structured-data format instead of the standard Junos format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see "Logging Messages in Structured-Data Format" on page 1489.
- A message's facility and severity level are together referred to as its *priority*. By default, the standard Junos format for messages does not include priority information (structured-data format includes a priority code by default.) To include priority information in standard-format messages directed to a file or a remote destination, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 1492.
- By default, the standard Junos format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see "Including the Year or Millisecond in Timestamps" on page 1496.
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by the Junos OS or messages generated on particular routers.
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote

destination. For more information, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

RELATED DOCUMENTATION

Examples: Configuring System Logging | 1502
Specifying the Facility and Severity of Messages to Include in the Log | 1527
Junos OS System Logging Facilities and Message Severity Levels | 1470
Directing System Log Messages to a Log File | 1530
Directing System Log Messages to a User Terminal | 1531
Directing System Log Messages to the Console | 1531

Overview of Single-Chassis System Logging Configuration

The Junos OS system logging utility on the QFX Series is similar to the UNIX **syslogd** utility. This topic describes how to configure system logging for a single-chassis system that runs the Junos OS.

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions. You always specify the facility and severity of the messages to include in the log. For more information, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

You direct messages to one or more destinations by including the appropriate statement at the **[edit system syslog]** hierarchy level:

- To a named file in a local file system, by including the **file** statement. See "Directing System Log Messages to a Log File" on page 1530.
- To the terminal session of one or more specific users (or all users) when they are logged in to the switch, by including the **user** statement. See "Directing System Log Messages to a User Terminal" on page 1531.
- To the switch console, by including the **console** statement. See "Directing System Log Messages to the Console" on page 1531.
- To a remote machine that is running the **syslogd** utility, by including the **host** statement. See "Directing System Log Messages to a Remote Machine" on page 1533.

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the *Junos OS System Log Messages Reference*. You can alter the content and format of logged messages in the following ways:

- You can log messages to a file in structured-data format instead of the standard Junos OS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see *Logging Messages in Structured-Data Format*.
- A message's facility and severity level are together referred to as its *priority*. By default, the standard Junos OS format for messages does not include priority information (structured-data format includes a priority code by default). To include priority information in standard-format messages directed to a file or a remote destination, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 1492.
- By default, the standard Junos OS format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see *Including the Year or Millisecond in Timestamps*.
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by Junos OS or messages generated on particular switches. For more information, see "Directing System Log Messages to a Remote Machine" on page 1533.
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination. For more information, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

> **NOTE:** During a commit check, warnings about the **traceoptions** configuration (for example, mismatch in trace file sizes or number of trace files) are not displayed on the console. However, these warnings are logged in the system log messages when the new configuration is committed.

RELATED DOCUMENTATION

Examples: Configuring System Logging

Specifying the Facility and Severity of Messages to Include in the Log | **1527**

Junos OS System Logging Facilities and Message Severity Levels | **1470**

Directing System Log Messages to a Log File | **1530**

Directing System Log Messages to a Remote Machine | **1533**

Directing System Log Messages to a User Terminal | 1531
Directing System Log Messages to the Console | 1531

Junos OS System Log Configuration Hierarchy

To configure the router to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string
        match "regular-expression";
        source-address source-address;
        structured-data {
            brief;
        }
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

Junos OS System Log Configuration Statements

To configure the switch to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites (ftp-url <password password>)> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host hostname {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

RELATED DOCUMENTATION

Overview of Junos OS System Log Messages | 1468

Junos OS Minimum System Logging Configuration

To record or view system log messages, you must include the **syslog** statement at the **[edit system]** hierarchy level. Specify at least one destination for the messages, as described in Table 151 on page 1486. For more information about the configuration statements, see "Single-Chassis System Logging Configuration Overview" on page 1480.

Table 151: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements

File	[edit system syslog]
	file *filename* {
	  facility severity;
	}

Terminal session of one, several, or all users	[edit system syslog]
	user (*username* | *) {
	  facility severity;
	}

Router or switch console	[edit system syslog]
	console {
	  facility severity;
	}

Remote machine or the other Routing Engine on the router or switch	[edit system syslog]
	host (*hostname* | other-routing-engine) {
	  facility severity;
	}

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

Example: Configuring System Log Messages

IN THIS SECTION

- Requirements | 1487
- Overview | 1487
- Configuration | 1488

The QFabric system monitors events that occur on its component devices and distributes system log messages about those events to all external system log message servers (hosts) that are configured. Component devices may include Node devices, Interconnect devices, Director devices, and the Virtual Chassis. Messages are stored for viewing only in the QFabric system database. To view the messages, issue the **show log** command.

This example describes how to configure system log messages on the QFabric system.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- QFabric system
- External servers that can be configured as system log message hosts

Overview

Component devices that generate system log message events may include Node devices, Interconnect devices, Director devices, and the control plane switches. The following configuration example includes these components in the QFabric system:

- Director software running on the Director group
- Control plane switches
- Interconnect device
- Multiple Node devices

Configuration

CLI Quick Configuration

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

```
set system syslog host 10.1.1.12 any error
set system syslog file qflogs
set system syslog file qflogs structured-data brief
set system syslog file qflogs archive size 1g
```

Step-by-Step Procedure

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

To configure system messages from the QFabric Director device:

1. Specify a host, any facility, and the **error** severity level.

```
[edit system syslog]
user@switch# set host 10.1.1.12 any error
```

> **NOTE:** You can configure more than one system log message server (host). The QFabric system sends the messages to each server configured.

2. (Optional) Specify a filename to capture log messages.

> **NOTE:** On the QFabric system, a syslog file named **messages** is configured implicitly with facility and severity levels of **any any** and a file size of 100 MBs. Therefore, you cannot specify the filename **messages** in your configuration, and automatic command completion does not work for that filename.

```
[edit system syslog]
user@switch# set file qflogs structured-data brief
user@switch# set file qflogs
```

3. (Optional) Configure the maximum size of your system log message archive file. This example specifies an archive size of 1 GB.

```
[edit system syslog]
user@switch# set file qflogs archive size 1g
```

Results

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

```
[edit]
user@switch# show system
syslog {
    file qflogs {
    }
    host 10.1.1.12 {
        any error;
    }
}
```

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

RELATED DOCUMENTATION

- *Understanding the Implementation of System Log Messages on the QFabric System*
- *syslog (QFabric System)*
- show log | **2936**

Logging Messages in Structured-Data Format

You can log messages to a file in structured-data format instead of the standard Junos OS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet standard RFC 5424, *The Syslog Protocol*, which is at https://tools.ietf.org/html/rfc5424. The RFC establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the **structured-data** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
    brief;
}
```

The optional **brief** statement suppresses the English-language text that appears by default at the end of a message to describe the error or event.

The structured format is used for all messages logged to the file that are generated by a Junos process or software library.

NOTE: If you include either or both of the **explicit-priority** and **time-format** statements along with the **structured-data** statement, they are ignored. These statements apply to the standard Junos OS system log format, not to structured-data format.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Specifying Log File Size, Number, and Archiving Properties

To prevent log files from growing too large, by default the Junos OS system logging utility writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for EX Series switches
- 1 megabyte (MB) for M Series, MX Series, and T Series routers
- 10 MB for TX Matrix or TX Matrix Plus routers
- 1 MB for the QFX Series

When an active log file called ***logfile*** reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file ***logfile*.0.gz**. The logging utility then opens and writes to a new active file called ***logfile***. This process is also known as file rotation. When the new ***logfile*** reaches the configured maximum size, ***logfile*.0.gz** is renamed ***logfile*.1.gz**, and the new ***logfile*** is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached and when the size of the active file reaches the configured maximum size, the contents of the last archived file are overwritten by the current active file. The logging utility by default also limits the users who can read log files to the **root** user and users who have Junos OS **maintenance** permission.

Junos OS provides a configuration statement **log-rotate-frequency** that configures the system log file rotation frequency by configuring the time interval for checking the log file size. The frequency can be set to a value of 1 minute through 59 minutes. The default frequency is 15 minutes.

To configure the log rotation frequency, include the **log-rotate-frequency** statement at the **[edit system syslog]** hierarchy level.

You can include the **archive** statement to change the maximum size of each file, how many archive files are created, and who can read log files.

To configure values that apply to all log files, include the **archive** statement at the **[edit system syslog]** hierarchy level:

```
archive <files number> <size size> <world-readable | no-world-readable>;
```

To configure values that apply to a specific log file, include the **archive** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
archive <archive-sites (ftp-url <password password>)> <files number> <size size> <start-time "YYYY-MM-DD.hh:mm">
    <transfer-interval minutes> <world-readable | no-world-readable> ;
```

archive-sites *site-name* specifies a list of archive sites that you want to use for storing files. The ***site-name*** value is any valid FTP URL to a destination. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the specified log filename. For information about how to specify valid FTP URLs, see Format for Specifying Filenames and URLs in Junos OS CLI Commands.

binary-data Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems). To restore the default setting, include the **no-binary-data** statement.

files *number* specifies the number of files to create before the oldest file is overwritten. The value can be from 1 through 1000.

size *size* specifies the maximum size of each file. The value can be from 64 KB (64k) through 1 gigabyte (1g); to represent megabytes, use the letter **m** after the integer. There is no space between the digits and the **k**, **m**, or **g** units letter.

start-time "*YYYY-MM-DD.hh:mm*" defines the date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval *interval* defines the amount of time the current log file remains open (even if it has not reached the maximum possible size) and receives new statistics before it is closed and transferred to an archive site. This interval value can be from 5 through 2880 minutes.

world-readable enables all users to read log files. To restore the default permissions, include the **no-world-readable** statement.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | **1480**

Examples: Configuring System Logging | **1502**

Routing Matrix with a TX Matrix Plus Router Solutions Page

Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```

NOTE: Messages logged in structured-data format include priority information by default. If you include the **structured-data** statement at the **[edit system syslog file *filename*]** hierarchy level along with the **explicit-priority** statement, the **explicit-priority** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 1489.

To include priority information in messages directed to a remote machine or the other Routing Engine, include the **explicit-priority** statement at the **[edit system syslog host (*hostname* | other-routing-engine)]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```

NOTE: The **other-routing-engine** option does not apply to the QFX Series.

The priority recorded in a message always indicates the original, local facility name. If the **facility-override** statement is included for messages directed to a remote destination, the Junos OS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 1536.

When the **explicit-priority** statement is included, the Junos OS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

```
FACILITY-severity[-TAG]
```

(The tag is a unique identifier assigned to some Junos OS system log messages.)

In the following example, the **CHASSISD_PARSE_COMPLETE** message belongs to the **daemon** facility and is assigned severity **info** (6):

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE: Using new configuration
```

When the **explicit-priority** statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new configuration
```

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

System Log Facility Codes and Numerical Codes Reported in Priority Information

Table 152 on page 1494 lists the facility codes that can appear in system log messages and maps them to facility names.

> **NOTE:** If the second column in Table 152 on page 1494 does not include the Junos OS facility name for a code, the facility cannot be included in a statement at the **[edit system syslog]** hierarchy level. Junos OS might use the facilities in Table 152 on page 1494—and others that are not listed—when reporting on internal operations.

Table 152: Facility Codes Reported in Priority Information

Code	Junos Facility Name	Type of Event or Error
AUTH	**authorization**	Authentication and authorization attempts
AUTHPRIV		Authentication and authorization attempts that can be viewed by superusers only
CHANGE	**change-log**	Changes to Junos OS configuration
CONFLICT	**conflict-log**	Specified configuration is invalid on the router type
CONSOLE		Messages written to **/dev/console** by the kernel console output r
CRON		Actions performed or errors encountered by the cron process
DAEMON	**daemon**	Actions performed or errors encountered by system processes
DFC	**dfc**	Actions performed or errors encountered by the dynamic flow capture process
FIREWALL	**firewall**	Packet filtering actions performed by a firewall filter
FTP	**ftp**	Actions performed or errors encountered by the FTP process

Table 152: Facility Codes Reported in Priority Information *(continued)*

Code	Junos Facility Name	Type of Event or Error
INTERACT	**interactive-commands**	Commands issued at the Junos OS CLI prompt or invoked by a client application such as a Junos XML protocol or NETCONF client
KERN	**kernel**	Actions performed or errors encountered by the Junos kernel
NTP		Actions performed or errors encountered by the Network Time Protocol (NTP)
PFE	**pfe**	Actions performed or errors encountered by the Packet Forwarding Engine
SYSLOG		Actions performed or errors encountered by the Junos system logging utility
USER	**user**	Actions performed or errors encountered by user-space processes

Table 153 on page 1495 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 153: Numerical Codes for Severity Levels Reported in Priority Information

Numerical Code	Severity Level	Description
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring
5	**notice**	Conditions that are not errors but might warrant special handling

Table 153: Numerical Codes for Severity Levels Reported in Priority Information *(continued)*

Numerical Code	Severity Level	Description
6	**info**	Events or nonerror conditions of interest
7	**debug**	Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level)

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | **1480**

Examples: Configuring System Logging | **1502**

Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To include the year, the millisecond, or both in the timestamp, include the **time-format** statement at the **[edit system syslog]** or **[edit security log]** hierarchy levels:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

The modified timestamp is used in messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

> **NOTE:** By default, in a FreeBSD console, the additional time information is not available in system log messages directed to each destination configured by a **host** statement. However, in a Junos OS specific implementation using the FreeBSD console, the additional time information is available in system log messages directed to each destination.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2006):

```
Aug 21 12:36:30.401 2006
```

> **NOTE:** Messages logged in structured-data format include the year and millisecond by default. If you include the structured-data statement at the **[edit system syslog file *filename*]** hierarchy level along with the **time-format** statement, the **time-format** statement is ignored and messages are logged in structured-data format.
>
> For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 1489.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Using Strings and Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also match messages against strings and regular expressions to refine which messages from a facility are logged to a file, a user terminal, or a remote destination.

The **match-strings** and **match** configuration statements enable you to match system log messages against a string or regular expression, respectively. You can include these statements at the following hierarchy levels:

- **[edit system syslog file *filename*]** (for a file)
- **[edit system syslog user (*username* | *)]** (for a specific user session or for all user sessions on a terminal)

- **[edit system syslog host (*hostname* | other-routing-engine)]** (for a remote destination)

To evaluate messages against a regular expression and only log matching messages to the given destination, include the **match** statement and specify the regular expression:

```
match "regular-expression";
```

Starting with Junos OS Release 16.1, you can use simple string comparisons to more efficiently filter messages, because it is less CPU-intensive than matching against complex regular expressions. To specify the text string that must appear in a message for the message to be logged to a destination, include the **match-strings** statement and specify the matching string or list of strings:

```
match-strings string-name;
```

```
match-strings [string1 string2];
```

The **match-strings** and **match** statements select messages with the configured facility and severity that match the given string or regular expression. The **match-strings** statement performs a simple string comparison, and as a result, it is less CPU-intensive than using the **match** statement to match against complex regular expressions. If you configure both the **match** and **match-strings** statements for the same destination, Junos OS evaluates the **match-strings** condition first; if the message includes any of the configured substrings, then the message is logged and the **match** condition is not evaluated. If the **match-strings** condition is not satisfied, then the system evaluates the message against the regular expression in the **match** configuration statement.

When specifying regular expressions for the **match** statement, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, http://www.ieee.org).

Table 154 on page 1498 specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term term refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.

> **NOTE:** The **match** statement is not case-sensitive.

Table 154: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.

Table 154: Regular Expression Operators for the match Statement *(continued)*

Operator	Matches
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
| (pipe)	One of the terms that appears on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS-specific.
^ (caret)	Start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Using Strings and Regular Expressions

Filter messages that belong to the **interactive-commands** facility, directing those that include the string **configure** to the terminal of the root user:

```
[edit system syslog]
user root {
 interactive-commands any;
 match-strings configure;
}
```

Messages like the following appear on the **root** user's terminal when a user issues a **configure** command to enter configuration mode:

```
timestamp router-name mgd[PID]: UI_CMDLINE_READ_LINE: User 'user', command 'configure private'
```

Filter messages that belong to the **daemon** facility and have a severity of **error** or higher, directing them to the file **/var/log/process-errors**. Omit messages generated by the SNMP process (snmpd), instead directing them to the file **/var/log/snmpd-errors**:

```
[edit system syslog]
file process-errors {
 daemon error;
 match "!(.*snmpd.*)";
}
file snmpd-errors {
 daemon error;
 match-strings snmpd;
}
```

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Junos System Log Regular Expression Operators for the match Statement

Table 155: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
| (pipe)	One of the terms that appear on either side of the pipe operator.

Table 155: Regular Expression Operators for the match Statement *(continued)*

Operator	Matches
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS–specific.
^ (caret)	The start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
$ (dollar sign)	The end of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, **[a-z0-9]** matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Disabling the System Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the ***facility* none** statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the **any *severity*** statement and then a ***facility* none** statement for each facility that you do not want to log. For example, the following logs all messages at the **error** level or higher to the console, except for messages from the **daemon** and **kernel** facilities. Messages from those facilities are logged to the file **>/var/log/internals** instead:

```
[edit system syslog]
console {
```

```
    any error;
    daemon none;
    kernel none;
}
file internals {
    daemon info;
    kernel info;
}
```

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging

The following example shows how to configure the logging of messages about all commands entered by users at the CLI prompt or invoked by client applications such as Junos OS XML protocol or NETCONF client applications, and all authentication or authorization attempts, both to the file **cli-commands** and to the terminal of any user who is logged in:

```
[edit system]
syslog {
    file cli-commands {
        interactive-commands info;
        authorization info;
    }
    user * {
        interactive-commands info;
        authorization info;
    }
}
```

The following example shows how to configure the logging of all changes in the state of alarms to the file **/var/log/alarms**:

```
[edit system]
syslog {
    file alarms {
```

```
        kernel warning;
    }
}
```

The following example shows how to configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user **alex**, to a remote machine, and to the console:

```
[edit system]
syslog {
    /* write all security-related messages to file /var/log/security */
    file security {
        authorization info;
        interactive-commands info;
    }
    /* write messages about potential problems to file /var/log/messages: */
    /* messages from "authorization" facility at level "notice" and above, */
    /* messages from all other facilities at level "warning" and above */
    file messages {
        authorization notice;
        any warning;
    }
    /* write all messages at level "critical" and above to terminal of user "alex" if */
    /* that user is logged in */
    user alex {
        any critical;
    }
    /* write all messages from the "daemon" facility at level "info" and above, and */
    /* messages from all other facilities at level "warning" and above, to the */
    /* machine monitor.mycompany.com */
    host monitor.mycompany.com {
        daemon info;
        any warning;
    }
    /* write all messages at level "error" and above to the system console */
    console {
        any error;
    }
}
```

The following example shows how to configure the handling of messages generated when users issue Junos OS CLI commands, by specifying the **interactive-commands** facility at the following severity levels:

- **info**—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file **/var/log/user-actions**.
- **notice**—Logs a message when users issue the configuration mode commands **rollback** and **commit**. The example writes the messages to the terminal of user **philip**.
- **warning**—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
    file user-actions {
        interactive-commands info;
    }
    user philip {
        interactive-commands notice;
    }
    console {
        interactive-commands warning;
    }
}
```

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Directing System Log Messages to a Log File | 1530

Examples: Assigning an Alternative Facility

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called **central-logger.mycompany.com**. The messages from California are assigned alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- Configure California routing platforms to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local0;
}
```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local2;
}
```

On **central-logger** you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

RELATED DOCUMENTATION

Alternate Facilities for System Log Messages Directed to a Remote Destination | **1538**

CHAPTER 47

Configuring System Logging for a TX Matrix or TX Matrix Plus Router

IN THIS CHAPTER

- Configuring System Logging for a TX Matrix Router | **1506**
- Configuring System Logging for a TX Matrix Plus Router | **1508**
- Configuring Message Forwarding to the TX Matrix Router | **1510**
- Configuring Message Forwarding to the TX Matrix Plus Router | **1512**
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router | **1513**
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router | **1516**
- Configuring Optional Features for Forwarded Messages on a TX Matrix Router | **1518**
- Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router | **1520**
- Configuring System Logging Differently on Each T640 Router in a Routing Matrix | **1522**
- Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix | **1524**

Configuring System Logging for a TX Matrix Router

To configure system logging for all routers in a routing matrix composed of a TX Matrix router and T640 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
```

```
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
        source-address source-address;
        port port number;
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

When included in the configuration on the TX Matrix router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix:

- **archive**—Sets the size and number of log files on each platform in the routing matrix. See "Specifying Log File Size, Number, and Archiving Properties" on page 1490.
- **console**—Directs the specified messages to the console of each platform in the routing matrix. See "Directing System Log Messages to the Console" on page 1531.
- **file**—Directs the specified messages to a file of the same name on each platform in the routing matrix. See "Directing System Log Messages to a Log File" on page 1530.
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

  The separate **match** statement at the **[edit system syslog host scc-master]** hierarchy level applies to messages forwarded from the T640 routers to the TX Matrix router. See "Configuring Optional Features for Forwarded Messages on a TX Matrix Router" on page 1518.
- **port**—Specifies the port number of the remote syslog server.

- **source-address**—Sets the IP address of the router to report in system log messages as the message source, when the messages are directed to the remote machines specified in all *hostname* statements at the **[edit system syslog]** hierarchy level, for each platform in the routing matrix. On a routing matrix composed of a TX Matrix router and T640 routers, the address is not reported by the T640 routers in messages directed to the other Routing Engine on each router or to the TX Matrix router. See "Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination" on page 1534.
- **structured-data**—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 1489.
- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 1496.
- **user**—Directs the specified messages to the terminal session of one or more specified users on each platform in the routing matrix that they are logged in to. See "Directing System Log Messages to a User Terminal" on page 1531.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

RELATED DOCUMENTATION

Configuring Message Forwarding to the TX Matrix Router | **1510**

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router | **1513**

Configuring Optional Features for Forwarded Messages on a TX Matrix Router | **1518**

Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router | **1541**

Configuring System Logging Differently on Each T640 Router in a Routing Matrix | **1522**

Configuring System Logging for a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

To configure system logging for all routers in a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs, include the **syslog** statement at the **[edit system]** hierarchy level on the SFC. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
```

```
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | sfc0-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

When included in the configuration on the TX Matrix Plus router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix.

- **archive**—Sets the size and number of log files on each router in the routing matrix. See "Specifying Log File Size, Number, and Archiving Properties" on page 1490.
- **console**—Directs the specified messages to the console of each router in the routing matrix. See "Directing System Log Messages to the Console" on page 1531.
- **file**—Directs the specified messages to a file of the same name on each router in the routing matrix. See "Directing System Log Messages to a Log File" on page 1530.
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

The separate **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level applies to messages forwarded from the T1600 or T4000 LCCs to the SFC. See "Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router" on page 1520.

- **source-address**—Sets the IP address of the router as the message source in system log messages when the messages are directed to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level, for each router in the routing matrix. On a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs, the address is not reported by the T1600 or T4000 routers in messages directed to the other Routing Engine on each router or to the TX Matrix Plus router. See "Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination" on page 1534.
- **structured-data**—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 1489.
- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 1496.
- **user**—Directs the specified messages to the terminal session of one or more specified users on each router in the routing matrix that they are logged in to. See "Directing System Log Messages to a User Terminal" on page 1531.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

RELATED DOCUMENTATION

Configuring Message Forwarding to the TX Matrix Plus Router | **1512**

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router | **1516**

Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router | **1520**

Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router | **1542**

Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix | **1524**

Routing Matrix with a TX Matrix Plus Router Solutions Page

Configuring Message Forwarding to the TX Matrix Router

By default, the master Routing Engine on each T640 router forwards to the master Routing Engine on the TX Matrix router all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host scc-master** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host scc-master {
    facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host scc-master {
    any none;
}
```

In either case, the setting applies to all T640 routers in the routing matrix.

To capture the messages forwarded by the T640 routers (as well as messages generated on the TX Matrix router itself), you must also configure system logging on the TX Matrix router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix router:

- To a file, as described in "Directing System Log Messages to a Log File" on page 1530.
- To the terminal session of one or more specific users (or all users), as described in "Directing System Log Messages to a User Terminal" on page 1531.
- To the console, as described in "Directing System Log Messages to the Console" on page 1531.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router" on page 1541.

As previously noted, the configuration statements included on the TX Matrix router also configure the same destinations on each T640 router in the routing matrix.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host scc-master]** hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Router | **1506**

Configuring Message Forwarding to the TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

By default, the master Routing Engine on each connected T1600 or T4000 LCC forwards to the master Routing Engine on the SFC all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host sfc0-master** statement at the **[edit system syslog]** hierarchy level on the SFC:

```
[edit system syslog]
host sfc0-master {
    facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host sfc0-master {
    any none;
}
```

In either case, the setting applies to all connected LCCs in the routing matrix.

To capture the messages forwarded by the T1600 or T4000 LCCs (as well as messages generated on the SFC itself), you must also configure system logging on the SFC. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the SFC:

- To a file, as described in "Directing System Log Messages to a Log File" on page 1530.
- To the terminal session of one or more specific users (or all users), as described in "Directing System Log Messages to a User Terminal" on page 1531.
- To the console, as described in "Directing System Log Messages to the Console" on page 1531.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router" on page 1542.

As previously noted, the configuration statements included on the SFC also configure the same destinations on each connected LCC.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host sfc0-master]** hierarchy level),

you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Plus Router | **1508**

Routing Matrix with a TX Matrix Plus Router Solutions Page

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router

IN THIS SECTION

- Messages Logged When the Local and Forwarded Severity Levels Are the Same | **1513**
- Messages Logged When the Local Severity Level Is Lower | **1514**
- Messages Logged When the Local Severity Level Is Higher | **1515**

This topic describes the impact of different local and forwarded severity levels configured for system log messages on a TX Matrix router:

Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix router contains all messages from the logs on the T640 routers. For example, you can specify severity **info** for the **/var/log/messages** file, which is the default severity level for messages forwarded by T640 routers:

```
[edit system syslog]
file messages {
    any info;
}
```

Table 156 on page 1514 specifies which messages are included in the logs on the T640 routers and the TX Matrix router.

Table 156: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**info**
TX Matrix router	Local	**info**
	Forwarded from T640 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix router, you can specify severity **notice** for the **/var/log/messages** file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
    any notice;
}
host scc-master {
    any critical;
}
```

Table 157 on page 1514 specifies which messages in a routing matrix are included in the logs on the T640 routers and the TX Matrix router. The T640 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix router does not include the messages with severity **error**, **warning**, or **notice** that the T640 routers log locally.

Table 157: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**notice**
TX Matrix router	Local	**notice**
	Forwarded from T640 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the **/var/log/messages** file and severity **notice** for forwarded messages:

```
[edit system syslog]
file messages {
    any critical;
}
host scc-master {
    any notice;
}
```

Table 158 on page 1515 specifies which messages are included in the logs on the T640 routers and the TX Matrix router. Although the T640 routers forward messages with severity **notice** and higher, the TX Matrix router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

Table 158: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**critical**
TX Matrix router	Local	**critical**
	Forwarded from T640 routers	**critical**

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Router | **1506**

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router

IN THIS SECTION

- Messages Logged When the Local and Forwarded Severity Levels Are the Same | 1516
- Messages Logged When the Local Severity Level Is Lower | 1517
- Messages Logged When the Local Severity Level Is Higher | 1517

This topic describes the impact of different local and forwarded severity levels configured for the system log messages on a TX Matrix Plus router:

Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix Plus router contains all messages from the logs on the T1600 routers in the routing matrix. For example, you can specify severity **info** for the **/var/log/messages** file, which is the default severity level for messages forwarded by T1600 routers:

```
[edit system syslog]
file messages {
    any info;
}
```

Table 159 on page 1516 specifies which messages in a routing matrix based on a TX Matrix Plus router are included in the logs on the T1600 routers and the TX Matrix Plus router:

Table 159: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**info**
TX Matrix Plus router	Local	**info**
	Forwarded from T1600 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix Plus router, you can specify severity **notice** for the **/var/log/messages** file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
    any notice;
}
host sfc0-master {
    any critical;
}
```

Table 160 on page 1517 specifies which messages in a routing matrix are included in the logs on the T1600 routers and the TX Matrix Plus router. The T1600 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix Plus router does not include the messages with severity **error**, **warning**, or **notice** that the T1600 routers log locally.

Table 160: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**notice**
TX Matrix Plus router	Local	**notice**
	Forwarded from T1600 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the **/var/log/messages** file and severity **notice** for forwarded messages:

```
[edit system syslog]
```

```
file messages {
    any critical;
}
host sfc0-master {
    any notice;
}
```

Table 161 on page 1518 specifies which messages are included in the logs on the T1600 routers and the TX Matrix Plus router. Although the T1600 routers forward messages with severity **notice** and higher, the TX Matrix Plus router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

Table 161: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**critical**
TX Matrix Plus router	Local	**critical**
	Forwarded from T1600 routers	**critical**

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Plus Router | **1508**

Configuring Optional Features for Forwarded Messages on a TX Matrix Router

To configure additional optional features when specifying how the T640 routers forward messages to the TX Matrix router, include statements at the **[edit system syslog host scc-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
```

```
host scc-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression";
}
```

You can also include the **facility-override** statement at the **[edit system syslog host scc-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix router, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 1536.

- Including Priority Information in Forwarded Messages | **1519**
- Adding a Text String to Forwarded Messages | **1520**
- Using Regular Expressions to Refine the Set of Forwarded Messages | **1520**

Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level, messages forwarded to the TX Matrix router include priority information. For the information to appear in a log file on the TX Matrix router, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the TX Matrix router. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host *hostname*]** hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router" on page 1541.

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix router also includes messages with those characteristics forwarded from the T640 routers.

```
[edit system syslog]
host scc-master {
    any notice;
    explicit-priority;
}
file messages {
    any notice;
```

```
    explicit-priority;
}
```

Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host scc-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix router. For more information, see "Adding a Text String to System Log Messages Directed to a Remote Destination" on page 1535.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host scc-master]** hierarchy level, the regular expression that you specify controls which messages from the T640 routers are forwarded to the TX Matrix router. The regular expression is not applied to messages from the T640 router that are directed to destinations other than the TX Matrix router. For more information about regular expression matching, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

SEE ALSO

Configuring System Logging for a TX Matrix Router | 1506

Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

To configure additional optional features when specifying how the connected T1600 or T4000 LCCs forward messages to the SFC, include statements at the **[edit system syslog host sfc0-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
```

```
host sfc0-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression;
}
```

You can also include the **facility-override** statement at the **[edit system syslog host sfc0-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the SFC, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 1536.

1. Including Priority Information in Forwarded Messages | 1521
2. Adding a Text String to Forwarded Messages | 1522
3. Using Regular Expressions to Refine the Set of Forwarded Messages | 1522

Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level, messages forwarded to the TX Matrix Plus router (or the SFC) include priority information. For the information to appear in a log file on the SFC, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the SFC. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host *hostname*]** hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router" on page 1542.

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix Plus router SFC also includes messages with those characteristics forwarded from the connected T1600 or T4000 LCCs.

```
[edit system syslog]
host sfc0-master {
    any notice;
    explicit-priority;
}
file messages {
    any notice;
```

```
    explicit-priority;
}
```

Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix Plus router. For more information, see "Adding a Text String to System Log Messages Directed to a Remote Destination" on page 1535.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the regular expression that you specify controls which messages from the connected T1600 or T4000 LCCs are forwarded to the TX Matrix Plus SFC. The regular expression is not applied to messages from the connected LCCs that are directed to destinations other than the SFC. For more information about regular expression matching, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

SEE ALSO

Configuring System Logging for a TX Matrix Plus Router | **1508**

Routing Matrix with a TX Matrix Plus Router Solutions Page

Configuring System Logging Differently on Each T640 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix router and T640 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix router:

- To configure settings that apply to the TX Matrix router but not the T640 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T640 routers, include them in the **lcc*n*-re0** and **lcc*n*-re1** configuration groups, where ***n*** is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T640 routers at any time.)

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T640 routers, because the **host scc-master** statement disables message forwarding.
- On the T640 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T640 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host scc-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
    system {
        syslog {
            file messages {
                authorization info;
```

```
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc1-re0 ...
}
```

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Router | 1506

Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix Plus router with T1600 or T4000 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix Plus router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix Plus router:

- To configure settings that apply to the TX Matrix Plus router but not the T1600 or T4000 routers, include them in the **re0** and **re1** configuration groups.

- To configure settings that apply to particular T1600 or T4000 routers, include them in the **lcc*n*-re0** and **lcc*n*-re1** configuration groups, where ***n*** is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T1600 or T4000 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T1600 or T4000 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *Junos OS CLI User Guide* .

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix Plus router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T1600 or T4000 routers, because the **host sfc0-master** statement disables message forwarding.
- On the T1600 or T4000 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T1600 or T4000 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host sfc0-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
    system {
        syslog {
            file messages {
                authorization info;
            }
```

```
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc1-re0 ...
}
```

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Plus Router | **1508**

Routing Matrix with a TX Matrix Plus Router Solutions Page

CHAPTER 48

Directing System Log Messages to a Remote Destination

IN THIS CHAPTER

- Specifying the Facility and Severity of Messages to Include in the Log | **1527**
- Directing System Log Messages to a Log File | **1530**
- Directing System Log Messages to a User Terminal | **1531**
- Directing System Log Messages to the Console | **1531**
- Directing System Log Messages to a Remote Machine or the Other Routing Engine | **1532**
- Directing System Log Messages to a Remote Machine | **1533**
- Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination | **1534**
- Adding a Text String to System Log Messages Directed to a Remote Destination | **1535**
- Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination | **1536**
- Default Facilities for System Log Messages Directed to a Remote Destination | **1538**
- Alternate Facilities for System Log Messages Directed to a Remote Destination | **1538**
- Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination | **1540**
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router | **1541**
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router | **1542**

Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a facility, which groups together messages that either are generated by the same source (such as a software process) or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level and higher are logged to the following destination:

```
[edit system syslog]
(console | file filename | host destination | user username) {
 facility severity ;
}
```

For more information about the destinations, see "Directing System Log Messages to a User Terminal" on page 1531, and, "Directing System Log Messages to the Console" on page 1531.

To log messages belonging to more than one facility to a particular destination, specify each facility and associated severity as a separate statement within the set of statements for the destination.

Table 147 on page 1470 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 162: Junos OS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Changes to the Junos OS configuration
conflict-log	Specified configuration is invalid on the router type
daemon	Actions performed or errors encountered by system processes
dfc	Events related to dynamic flow capture
explicit-priority	Include priority and facility in system log messages
external	Actions performed or errors encountered by the local external applications
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
kernel	Actions performed or errors encountered by the Junos OS kernel

Table 162: Junos OS System Logging Facilities *(continued)*

Facility	Type of Event or Error
ntp	Actions performed or errors encountered by the Network Time Protocol processes
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
security	Security related events or errors
user	Actions performed or errors encountered by user-space processes

Table 148 on page 1471 lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see "Disabling the System Logging of a Facility" on page 1501.

Table 163: System Log Message Severity Levels

Value	Severity Level	Description
N/A	**none**	Disables logging of the associated facility to a destination
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring
5	**notice**	Conditions that are not errors but might warrant special handling
6	**info**	Events or nonerror conditions of interest
7	**any**	Includes all severity levels

RELATED DOCUMENTATION

Junos OS System Logging Facilities and Message Severity Levels | 1470

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Directing System Log Messages to a Log File

To direct system log messages to a file in the **/var/log** directory of the local Routing Engine, include the **file** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
file filename {
    facility severity;
    archive <archive-sites (ftp-url <password password>)> <files number> <size size>
        <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
        brief;
    }
}
```

For the list of facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

To prevent log files from growing too large, the Junos OS system logging utility by default writes messages to a sequence of files of a defined size. By including the **archive** statement, you can configure the number of files, their maximum size, and who can read them, either for all log files or for a certain log file. For more information, see "Specifying Log File Size, Number, and Archiving Properties" on page 1490.

For information about the following statements, see the indicated sections:

- **explicit-priority**—See "Including Priority Information in System Log Messages" on page 1492
- **match**—See "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497
- **structured-data**—See "Logging Messages in Structured-Data Format" on page 1489

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Overview of Junos OS System Log Messages | 1468

Logging Messages in Structured-Data Format | 1489

Examples: Configuring System Logging | 1502

Directing System Log Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the **user** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
user (username | *) {
    facility severity;
    match "regular-expression";
}
```

Specify one or more Junos OS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527. For information about the **match** statement, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Directing System Log Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the **console** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
console {
    facility severity;
}
```

For the list of logging facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Examples: Configuring System Logging | 1502

Directing System Log Messages to a Remote Machine or the Other Routing Engine

To direct system log messages to a remote machine or to the other Routing Engine on the router, include the **host** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
source-address source-address;
```

To direct system log messages to a remote machine, include the **host** *hostname* statement to specify the remote machine's IP version 4 (IPv4) address, IP version 6 (IPv6) address, or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks router. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

To direct system log messages to the other Routing Engine on a router with two Routing Engines installed and operational, include the **host other-routing-engine** statement. The statement is not automatically reciprocal, so you must include it in each Routing Engine configuration if you want the Routing Engines to direct messages to each other. In each message directed to the other Routing Engine, the string **re0** or **re1** appears after the timestamp to indicate the source for the message.

To record facility and severity level information in each message, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 1492.

For information about the **match** statement, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the router that is reported in the messages as their source. In each **host** statement, include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message. You can include the **structured-data** statement to enable the forwarding of structured system log messages to a remote system log server in the IETF system log message format.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Directing System Log Messages to a Remote Machine

To direct system log messages to a remote machine, include the **host** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

To direct system log messages to a remote machine, include the **host *hostname*** statement to specify the remote machine's IP version 4 (IPv4) address or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks switch. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

For the list of logging facilities and severity levels to configure under the **host** statement, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

To record facility and severity level information in each message, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 1492.

For information about the **match** statement, see "Using Strings and Regular Expressions to Refine the Set of Logged Messages" on page 1497.

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the switch that is reported in the messages as their source. In each **host** statement, you can also include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message.

RELATED DOCUMENTATION

Overview of Single-Chassis System Logging Configuration | **1482**

Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination

To specify the source router to be reported in system log messages when the messages are directed to a remote machine, include the **source-address** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
source-address source-address;
```

source-address is a valid IPv4 or IPv6 address configured on one of the router interfaces. The address is reported in the messages directed to all remote machines specified in **host *hostname*** statements at the **[edit system syslog]** hierarchy level, but not in messages directed to the other Routing Engine.

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | **1480**

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination | **1540**

Adding a Text String to System Log Messages Directed to a Remote Destination

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the **log-prefix** statement at the **[edit system syslog host]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign (=) and the colon (:). It also cannot include the space character; do not enclose the string in quotation marks (“ ”) in an attempt to include spaces in it.

The Junos OS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

The following example shows how to add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine hardware-logger.mycompany.com:

```
[edit system syslog]
host hardware-logger.mycompany.com {
    any info;
    log-prefix M120;
}
```

When these configuration statements are included on an M120 router called origin1, a message in the system log on hardware-logger.mycompany.com looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user ‘root’, command ‘run show version’
```

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Specifying Log File Size, Number, and Archiving Properties | 1490

Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination

Some facilities assigned to messages logged on the local router or switch have Junos OS-specific names (see Table 147 on page 1470). In the recommended configuration, a remote machine designated at the **[edit system syslog host *hostname*]** hierarchy level is not a Juniper Networks router or switch, so its syslogd utility cannot interpret the Junos OS-specific names. To enable the standard syslogd utility to handle messages from these facilities when messages are directed to a remote machine, a standard **local*X*** facility name is used instead of the Junos OS-specific facility name.

Table 164 on page 1538 lists the default alternative facility name next to the Junos OS-specific facility name it is used for.

The syslogd utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks router or switch or the remote machine itself). For example, the following statements in the configuration of the router called **local-router** direct messages from the **authorization** facility to the remote machine *monitor.mycompany.com*:

```
[edit system syslog]
host monitor.mycompany.com {
    authorization info;
}
```

The default alternative facility for the local **authorization** facility is also **authorization**. If the syslogd utility on **monitor** is configured to write messages belonging to the **authorization** facility to the file **/var/log/auth-attempts**, then the file contains the messages generated when users log in to **local-router** and the messages generated when users log in to **monitor**. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the **auth-attempts** file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on **local-router** when they are directed to **monitor**. You can then configure the syslogd utility on **monitor** to write messages with the alternative facility to a different file from messages generated on **monitor** itself.

To change the facility used for all messages directed to a remote machine, include the **facility-override** statement at the **[edit system syslog host *hostname*]** hierarchy level:

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the **local*X*** facilities. On the remote machine, you must also configure the syslogd utility to handle the messages in the desired manner.

Table 165 on page 1539 lists the facilities that you can specify in the **facility-override** statement.

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

The following example shows how to log all messages generated on the local router at the error level or higher to the local0 facility on the remote machine called monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

The following example shows how to configure routers located in California and routers located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned to alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routers to aggregate messages in the local0 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local0;
  }
  ```

- Configure New York routers to aggregate messages in the local2 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local2;
  }
  ```

On central-logger, you can then configure the system logging utility to write messages from the local0 facility to the file **change-log** and the messages from the local2 facility to the file **new-york-config**.

RELATED DOCUMENTATION

Table 164 | 1538

Alternate Facilities for System Log Messages Directed to a Remote Destination | 1538

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination | 1540

Default Facilities for System Log Messages Directed to a Remote Destination

Table 164 on page 1538 lists the default alternative facility name next to the Junos OS-specific facility name for which it is used. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 164: Default Facilities for Messages Directed to a Remote Destination

Junos OS–Specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7
pfe	local4

RELATED DOCUMENTATION

Single-Chassis System Logging Configuration Overview | 1480

Alternate Facilities for System Log Messages Directed to a Remote Destination

Table 165 on page 1539 lists the facilities that you can specify in the **facility-override** statement.

Table 165: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the Junos OS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by user-space processes

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

RELATED DOCUMENTATION

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination | **1540**

Single-Chassis System Logging Configuration Overview | **1480**

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routing platforms to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local0;
}
```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local2;
}
```

On **central-logger,** you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

RELATED DOCUMENTATION

Alternate Facilities for System Log Messages Directed to a Remote Destination | **1538**

Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router

You can configure a routing matrix composed of a TX Matrix router and T640 routers to direct system logging messages to a remote machine or the other Routing Engine on each router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

The TX Matrix router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system.

For the TX Matrix router to include priority information when it directs messages that originated on a T640 router to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the T640 routers to the TX Matrix router. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each T640 router sends messages to the **re1** Routing Engine on its platform only. It does not also send messages directly to the **re1** Routing Engine on the TX Matrix router.

Because the configuration on the TX Matrix router applies to the T640 routers, any T640 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routers are configured to forward messages to the TX Matrix router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 router and the other from the TX Matrix router. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see “Configuring Message Forwarding to the TX Matrix Router” on page 1510.
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single router.

- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Router | 1506

Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers also called the ine-card chassis LCC) in the routing matrix.

You can configure a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs to direct system logging messages to a remote machine or the other Routing Engine on each routing router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the SFC:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

The TX Matrix Plus router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system.

For the TX Matrix Plus router to include priority information when it directs messages that originated on a connected T1600 or T4000 LCC to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the connected T1600 or T4000 LCCs to the SFC. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each connected T1600 or T4000 LCC sends messages

to the **re1** Routing Engine on its router only. It does not also send messages directly to the **re1** Routing Engine on the SFC.

Because the configuration on the SFC applies to the connected T1600 or T4000 LCCs, any LCC that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the LCCs are configured to forward messages to the SFC (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T1600 or T4000 LCC and the other from the SFC. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see "Configuring Message Forwarding to the TX Matrix Plus Router" on page 1512.
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single routing router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

RELATED DOCUMENTATION

Configuring System Logging for a TX Matrix Plus Router | **1508**

Routing Matrix with a TX Matrix Plus Router Solutions Page

CHAPTER 49

Displaying System Log Files

IN THIS CHAPTER

- Displaying a Log File from a Single-Chassis System | **1544**
- Log File Sample Content | **1545**
- Displaying a Log File from a Routing Matrix | **1546**

Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue either of the following commands:

```
user@host> show log log-filename
user@host> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine. To display the file stored on a particular Routing Engine, prefix the file or pathname with the string **re0** or **re1** and a colon. The following examples both display the **/var/log/messages** file stored on the Routing Engine in slot 1:

```
user@host> show log re1:messages
user@host> file show re1:/var/log/messages
```

For information about the fields in a log message, see "Interpreting Messages Generated in Standard Format by a Junos OS Process or Library" on page 1554, "Interpreting Messages Generated in Standard Format by Services on a PIC" on page 1555, and "Interpreting Messages Generated in Structured-Data Format" on page 1556. For examples, see "Log File Sample Content" on page 1545.

Log File Sample Content

This topic contains sample content from the /var/log directory. You can display the contents of the **/var/log/messages** file stored on the local Routing Engine. (The **/var/log** directory is the default location for log files, so you do not need to include it in the filename. The **messages** file is a commonly configured destination for system log messages.)

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]: UI_DBASE_LOGIN_EVENT: User 'barbara'
    entering configuration mode
Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara' exiting configuration mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no comment
Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82, ifAdminStatus up(1), ifOperStatus
    down(2), ifName at-1/0/0
```

You can display the contents of the file **/var/log/processes**, which has been previously configured to include messages from the **daemon** facility. When issuing the **file show** command, you must specify the full pathname of the file:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]: SNMPD_TRAP_WARM_START:
    trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler:
    cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
    start
Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

You can display the contents of the file **/var/log/processes** when the **explicit-priority** statement is included at the [**edit system syslog file processes**] hierarchy level:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

Warning Message Support for Throughput Overuse:

The SRX4100 device supports up to 20 Gbps and 7 Mpps of Internet mix (IMIX) firewall performance. When IMIX throughput exceeds 20 Gbps and 7 Mpps on an SRX4100 device, new log messages are logged.

These log messages remind you that there is throughput overuse. You can see the following sample log messages when you issue the **show log messages** command.

```
user@host> show log messages
Apr 25 14:01:12 user Throughput exceed 20Gbps and 7Mpps in 35% of last 15 minutes, above the time threshold
   10%!
Apr 25 14:16:12 user Throughput exceed 20Gbps and 7Mpps in 95% of last 15 minutes, above the time threshold
   10%!
```

As a reminder of throughput overuse, every 15 minutes the system calculates how many minutes the throughout has exceeded 20 Gbps and 7 Mpps. The system triggers a log message if the throughput has exceeded more than 1 minute, 30 seconds (10%) of the last 15 minutes. For example, suppose you see the following log message:

```
Throughput exceed 20 Gbps and 7 Mpps in 35% of last 15 minutes, above the time
threshold 10%!
```

It means your throughput has exceeded 20 Gbps and 7 Mpps for 5 minutes, 15 seconds of the last 15 minutes (35% of 15 minutes) that triggered the log message.

To turn off this log message, we recommend that you bring down the throughput level below 20 Gbps and 7 Mpps or install the enhanced performance upgrade license.

NOTE: This feature requires a license. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Services Gateways for details, or contact your Juniper Account Team or Juniper Partner.

Displaying a Log File from a Routing Matrix

One way to display a log file stored on the local Routing Engine of any of the individual platforms in a routing matrix (T640 routing nodes or TX Matrix platform) is to log in to a Routing Engine on the platform, enter Junos OS CLI operational mode, and issue the **show log** or **file show** command described in "Displaying a Log File from a Single-Chassis System" on page 1544.

To display a log file stored on a T640 routing node during a terminal session on the TX Matrix platform, issue the **show log** or **file show** command and add a prefix that specifies the T640 routing node's LCC index number as lccn, followed by a colon. The index can be from 0 (zero) through 3:

```
user@host> show log lccn:log-filename
user@host> file show lccn:log-file-pathname
```

By default, the **show log** and **file show** commands display the specified log file stored on the master Routing Engine on the T640 routing node. To display the log from a particular Routing Engine, prefix the file- or pathname with the string lccn-master, **lccn-re0**, or **lccn-re1**, followed by a colon. The following examples all display the **/var/log/messages** file stored on the master Routing Engine (in slot 0) on routing node LCC2:

```
user@host> show log lcc2:messages
user@host> show log lcc2-master:messages
user@host> show log lcc2-re0:messages
user@host> file show lcc2:/var/log/messages
```

If the T640 routing nodes are forwarding messages to the TX Matrix platform (as in the default configuration), another way to view messages generated on a T640 routing node during a terminal session on the TX Matrix platform is simply to display a local log file. However, the messages are intermixed with messages from other T640 routing nodes and the TX Matrix platform itself. For more information about message forwarding, see "Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router" on page 1513.

For information about the fields in a log message, see "Interpreting Messages Generated in Structured-Data Format" on page 1556, "Interpreting Messages Generated in Standard Format by Services on a PIC" on page 1555, and "Interpreting Messages Generated in Standard Format by a Junos OS Process or Library" on page 1554. For examples, see "Log File Sample Content" on page 1545.

CHAPTER 50

Displaying and Interpreting System Log Message Descriptions

IN THIS CHAPTER

- Displaying and Interpreting System Log Message Descriptions | **1548**
- The message-source Field on a Single-Chassis System | **1550**
- The message-source Field on a TX Matrix Platform | **1551**
- The message-source Field on a T640 Routing Node in a Routing Matrix | **1553**
- Interpreting Messages Generated in Standard Format by a Junos OS Process or Library | **1554**
- Interpreting Messages Generated in Standard Format by Services on a PIC | **1555**
- Interpreting Messages Generated in Structured-Data Format | **1556**
- Examples: Displaying System Log Message Descriptions | **1561**

Displaying and Interpreting System Log Message Descriptions

This reference lists the messages available at the time of its publication. To display the list of messages that applies to the version of Junos OS that is running on a routing platform, enter the Junos OS CLI operational mode and issue the following command:

```
user@host> help syslog ?
```

To display the list of available descriptions for tags whose names begin with a specific character string, substitute the string (in all capital letters) for the variable ***TAG-PREFIX*** (there is no space between the prefix and the question mark):

```
user@host> help syslog TAG-PREFIX?
```

To display the complete descriptions for tags whose name includes a regular expression, substitute a Perl-based expression for the variable regex. The match is not case-sensitive. For information about Perl-based regular expressions, consult a Perl reference manual or website such as http://perldoc.perl.org.

```
user@host> help syslog regex
```

To display the complete description of a particular message, substitute its name for the variable ***TAG*** (in all capital letters):

```
user@host> help syslog TAG
```

Table 166 on page 1549 describes the fields in a system log message description in this reference or in the CLI.

Table 166: Fields in System Log Message Descriptions

Field Name in Reference	Field Name in CLI	Description
—	**Name**	The message tag in all capital letters.
System Log Message	**Message**	Text of the message written to the system log. In the log, a specific value is substituted for each variable that appears in italics in this reference or in angle brackets (<>) in the CLI. In this reference, the message text appears on the second line of the **System Log Message** field. The first line is the message tag (the same text as in the **CLI** Name field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error.
—	**Help**	Short description of the message, which also appears in the right-hand column of CLI output for the **help syslog** command when the output lists multiple messages.
Description	**Description**	More detailed explanation of the message.

Table 166: Fields in System Log Message Descriptions *(continued)*

Field Name in Reference	Field Name in CLI	Description
Type	**Type**	Category to which the message belongs: • **Error**: The message reports an error or failure condition that might require corrective action. • **Event**: The message reports a condition or occurrence that does not generally require corrective action.
Severity	**Severity**	Message severity level as described in Table: **System Log Message Severity Levels** in "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.
Cause	**Cause**	(Optional) Possible cause for message generation. There can be more than one cause.
Action	**Action**	(Optional) Action you can perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.

The message-source Field on a Single-Chassis System

The format of the ***message-source*** field in a message on a single-chassis system depends on whether the message was generated on the local Routing Engine or the other Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.

- When the local Routing Engine generated the message, there are two subfields:

```
hostname process[process-ID]
```

- When the other Routing Engine generated the message, there are three subfields:

```
hostname reX process[process-ID]
```

hostname is the hostname of the local Routing Engine.

process[process-ID] is the name and PID of the process that generated the message. If the **reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [*process-ID*] part does not appear.

reX indicates that the other Routing Engine generated the message (***X*** is 0 or 1).

The message-source Field on a TX Matrix Platform

The format of the *message-source* field in a message on a TX Matrix platform depends on several factors:

- Whether the message was generated on the TX Matrix platform or a T640 routing node in the routing matrix. By default, the master Routing Engine on each T640 routing node forwards messages from all facilities with severity info and higher to the master Routing Engine on the TX Matrix platform. When you configure system logging on the TX Matrix platform, its logs include the forwarded messages. For more information, see "Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router" on page 1513.
- Whether the message was generated on the local Routing Engine or the other Routing Engine on the originating machine (TX Matrix platform or T640 routing node). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 167 on page 1552 specifies the format of the message-source field in the various cases.

Table 167: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Machine	Generating Routing Engine	Process or Component	Format
TX Matrix platform	Local	Process	***hostname process[processID]***
		Component	***hostname scc-reX process[processID]***
	Other	Process	***hostname scc-reX scc-componentZ process***
		Component	***hostname scc-reX scc-componentZ process***
T640 routing node	Local	Process	***hostname lccY-masterprocess[processID]***
		Component	***hostname lccY-master scc-componentZ process***
	Other	Process	***hostname lccY-master lccY-reX process[processID]***
		Component	***hostname lccY-master lccY-reX lccY-componentZ process***

hostname is the hostname of the local Routing Engine on the TX Matrix platform.

lccY*-master** is the master Routing Engine on the T640 routing node with the indicated LCC index number (Y*** is from 0 through 3).

lccY-reX indicates that the backup Routing Engine on the T640 routing node generated the message (***X*** is 0 or 1). The routing node has the indicated LCC index number (***Y*** matches the value in the **lccY-master** field.

lccY-componentZ process identifies the hardware component and process on the T640 routing node that generated the message (***Y*** matches the value in the **lccY-master** field and the range of values for ***Z*** depends on the component type). For example, **lcc2-fpc1 PFEMAN** refers to a process on the FPC in slot 1 on the T640 routing node with index LCC2.

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the **scc-reX** or **lccY-reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [***process-ID***] part does not appear.

scc-componentZ process identifies the hardware component and process on the TX Matrix platform that generated the message (the range of values for ***Z*** depends on the component type). For example, **spmb1 GSIB** refers to a process on one of the processor boards in the Switch Interface Board (SIB) with index 1.

scc-reX indicates that the other Routing Engine on the TX Matrix platform generated the message (***X*** is 0 or 1).

The message-source Field on a T640 Routing Node in a Routing Matrix

The format of the ***message-source*** field in a message on a T640 routing node in a routing matrix depends on two factors:

- Whether the message was generated on the local Routing Engine or the other Routing Engine. Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 168 on page 1553 specifies the format of the ***message-source*** field in the various cases.

Table 168: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Routing Engine	Process or Component	Format
Local	Process	***hostname-lccY process[processID]***
	Component	***hostname-lccY lccY-componentZ process***
Other	Process	***hostname-lccY lccY-reX process[processID]***
	Component	***hostname-lccY lccY-reX lccY-componentZ process***

hostname-lccY is the hostname of the local Routing Engine and the T640 routing node's LCC index number.

lccY-componentZ process identifies the hardware component and process that generated the message (***Y*** matches the value in the ***hostname-lccY*** field and the range of values for ***Z*** depends on the component type). For example, lcc0-fpc0 CMLC refers to a process on the FPC in slot 0. The T640 routing node has index LCC0 in the routing matrix.

lccY-reX indicates that the other Routing Engine on the routing node generated the message (***Y*** matches the value in the ***hostname-lccY*** field and ***X*** is 0 or 1).

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the ***lccY-reX*** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [***process-ID***] part does not appear.

Interpreting Messages Generated in Standard Format by a Junos OS Process or Library

The syntax of a standard-format message generated by a Junos OS process or subroutine library depends on whether it includes priority information:

- When the **explicit-priority** statement is included at the [**edit system syslog file *filename***] or [**edit system syslog host (*hostname* | other-routing-engine)**] hierarchy level, a system log message has the following syntax:

```
timestamp  message-source: %facility-severity-TAG: message-text
```

- When directed to the console or to users, or when the **explicit-priority** statement is not included for files or remote hosts, a system log message has the following syntax:

```
timestamp  message-source: TAG: message-text
```

Table 169 on page 1554 describes the message fields.

Table 169: Fields in Standard-Format Messages Generated by a Junos OS process or Library

Field	Description
timestamp	Time at which the message was logged.
message-source	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields, depending on how system logging is configured. See "The message-source Field on a TX Matrix Platform" on page 1551,"The message-source Field on a T640 Routing Node in a Routing Matrix" on page 1553, and "The message-source Field on a Single-Chassis System" on page 1550.
facility	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: *Numerical Codes for Severity Levels Reported in Priority Information* in "Including Priority Information in System Log Messages" on page 1492.

Table 169: Fields in Standard-Format Messages Generated by a Junos OS process or Library *(continued)*

Field	Description
severity	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table: *Numerical Codes for Severity Levels Reported in Priority Information* in "Including Priority Information in System Log Messages" on page 1492.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix. Not all processes on a routing platform use tags, so this field does not always appear.
message-text	Text of the message. For the text for each message, see the chapters following System Log Messages.

Interpreting Messages Generated in Standard Format by Services on a PIC

Standard-format system log messages generated by services on a PIC, such as the Adaptive Services (AS) PIC, have the following syntax:

```
timestamp  (FPC Slot fpc-slot, PIC Slot pic-slot) {service-set} [SERVICE]:
 optional-string TAG: message-text
```

NOTE: System logging for services on PICs is not configured at the [**edit system syslog**] hierarchy level as discussed in this chapter. For configuration information, see the *Junos Services Interfaces Configuration Guide*.

The (**FPC Slot *fpc-slot***, **PIC Slot *pic-slot***) field appears only when the standard system logging utility that runs on the Routing Engine writes the messages to the system log. When the PIC writes the message directly, the field does not appear.

Table 170 on page 1556 describes the message fields.

Table 170: Fields in Messages Generated by a PIC

Field	Description
timestamp	Time at which the message was logged.
fpc-slot	Slot number of the Flexible PIC Concentrator (FPC) that houses the PIC that generated the message.
pic-slot	Number of the PIC slot on the FPC in which the PIC that generated the message resides.
service-set	Name of the service set that generated the message.
SERVICE	Code representing the service that generated the message. The codes include the following: • FWNAT—Network Address Translation (NAT) service • IDS—Intrusion detection service
optional-string	A text string that appears if the configuration for the PIC includes the log-prefix statement at the [edit interfaces interface-name services-options syslog] hierarchy level. For more information, see the *Junos Services Interfaces Configuration Guide*.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating PIC. The entries in this reference are ordered alphabetically by this prefix.
message-text	Text of the message. For the text of each message, see System Log Messages.

Interpreting Messages Generated in Structured-Data Format

Beginning in Junos OS Release 8.3, when the **structured-data** statement is included in the configuration for a log file, Junos OS processes and software libraries write messages to the file in structured-data format instead of the standard Junos OS format. For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 1489.

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values. In standard format, the variables are interspersed in the message text and not identified as variables.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

<priority code>version timestamp hostname process processID TAG [junos@2636.platform variable-value-pairs] message-text

Table 171 on page 1557 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 171: Fields in Structured-Data Messages

Field	Description	Examples
<priority code>	Number that indicates the message's facility and severity. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see Table: **Facility and Severity Codes in the priority-code Field** in "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.	<165> for a message from the **pfe** facility (facility=20) with severity **notice** (severity=5).
version	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version
timestamp	Time when the message was generated, in one of two representations: • ***YYYY-MM-DDTHH:MM:SS.MSZ*** is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC) • ***YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM*** is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719 -08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	3046
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT

Table 171: Fields in Structured-Data Messages *(continued)*

Field	Description	Examples
junos@2636.platform	An identifier for the type of hardware platform that generated the message. The junos@2636 prefix indicates that the platform runs Junos OS. It is followed by a dot-separated numerical identifier for the platform type. For a list of the identifiers, see Table 173 on page 1560.	junos@2636.1.1.1.2.18 for the M120 router
variable-value-pairs	A variable-value pair for each element in the *message-text* string that varies depending on the circumstances that triggered the message. Each pair appears in the format ***variable = "value"***.	username="user"
message-text	English-language description of the event or error (omitted if the brief statement is included at the [**edit system syslog file *filename* structured-data**] hierarchy level). For the text for each message, see the chapters following System Log Messages.	User 'user' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT [junos@2636.1.1.1.2.18
    username="user"] User 'user' exiting configuration mode
```

When the brief statement is included at the [**edit system syslog file *filename* structured-data**] hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT [junos@2636.1.1.1.2.18
    username="user"]
```

Table 172 on page 1559 maps the codes that appear in the ***priority-code*** field to facility and severity level.

NOTE: Not all of the facilities and severities listed in Table 172 on page 1559 can be included in statements at the [**edit system syslog**] hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 1527.

Table 172: Facility and Severity Codes in the priority-code Field

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103
security (13)	104	105	106	107	108	109	110	111
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167

Table 172: Facility and Severity Codes in the priority-code Field *(continued)*

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Table 173 on page 1560 lists the numerical identifiers for routing platforms that appear in the ***platform*** field. The identifier is derived from the platform's SNMP object identifier (OID) as defined in the Juniper Networks routing platform MIB. For more information about OIDs, see the *Network Management and Monitoring Guide*.

Table 173: Platform Identifiers in the platform Field

Identifier	Platform Name
1.1.1.2.1	M40 router
1.1.1.2.2	M20 router
1.1.1.2.3	M160 router
1.1.1.2.4	M10 router
1.1.1.2.5	M5 router
1.1.1.2.6	T640 routing node
1.1.1.2.7	T320 router
1.1.1.2.8	M40e router
1.1.1.2.9	M320 router
1.1.1.2.10	M7i router
1.1.1.2.11	M10i router
1.1.1.2.13	J2300 Services Router
1.1.1.2.14	J4300 Services Router

Table 173: Platform Identifiers in the platform Field *(continued)*

Identifier	Platform Name
1.1.1.2.15	J6300 Services Router
1.1.1.2.17	TX Matrix platform
1.1.1.2.18	M120 router
1.1.1.2.19	J4350 Services Router
1.1.1.2.20	J6350 Services Router
1.1.1.2.23	J2320 Services Router
1.1.1.2.24	J2350 Services Router
1.1.1.2.27	T1600 router
1.1.1.2.37	TX Matrix Plus platform
1.1.1.2.83	T4000 router

Examples: Displaying System Log Message Descriptions

Display the list of all currently available system log message descriptions:

```
user@host> help syslog ?
```

```
Possible completions:
<syslog-tag>   Syslog tag
 . . .      . . .
BOOTPD_ARG_ERR   Command-line option was invalid
BOOTPD_BAD_ID   Request failed because assembly ID was unknown
BOOTPD_BOOTSTRING  tnp.bootpd provided boot string
BOOTPD_CONFIG_ERR  tnp.bootpd could not parse configuration file;
       used default settings
BOOTPD_CONF_OPEN  tnp.bootpd could not open configuration file
BOOTPD_DUP_REV   Extra boot string definitions for revision were
```

```
       ignored
---(more 4%)---
```

Display the list of all currently available system log message descriptions for tags that begin with the letters **ACCT** (there is no space between **ACCT** and the question mark, and some descriptions are shortened for legibility):

```
user@host> help syslog ACCT?
```

```
Possible completions:
<syslog-tag>       System log tag or regular expression
ACCT_ACCOUNTING_FERROR    Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR   Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE Maximum file size is smaller than ...
ACCT_BAD_RECORD_FORMAT    Record format does not match accounting profile
ACCT_CU_RTSLIB_ERROR    Error occurred obtaining current class usage ...
ACCT_FORK_ERR       Could not create child process
ACCT_FORK_LIMIT_EXCEEDED   Could not create child process because of limit
ACCT_GETHOSTNAME_ERROR    gethostname function failed
ACCT_MALLOC_FAILURE     Memory allocation failed
ACCT_UNDEFINED_COUNTER_NAME  Filter profile used undefined counter name
ACCT_XFER_FAILED      Attempt to transfer file failed
ACCT_XFER_POPEN_FAIL    File transfer failed
```

Display the description of the **UI_CMDLINE_READ_LINE** message:

```
user@host> help syslog UI_CMDLINE_READ_LINE
```

```
Name:    UI_CMDLINE_READ_LINE
Message:   User '<users>', command '<input>'
Help:    User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI
     prompt and pressed the Enter key, sending the command string
     to the management process (mgd).
Type:    Event: This message reports an event, not an error
Severity:   info
```

CHAPTER 51

Configuring System Logging for a Security Device

IN THIS CHAPTER

- Understanding System Logging for Security Devices | 1563
- Understanding Stream Logging for Security Devices | 1565
- Understanding Binary Format for Security Logs | 1566
- Understanding On-Box Logging and Reporting | 1568
- Monitoring Reports | 1574
- Configuring On-Box Binary Security Log Files | 1582
- Configuring Off-Box Binary Security Log Files | 1584
- Sending System Log Messages to a File | 1586
- Setting the System to Send All Log Messages Through eventd | 1586
- Setting the System to Stream Security Logs | 1587

Understanding System Logging for Security Devices

IN THIS SECTION

- Control Plane and Data Plane Logs | 1564
- Redundant System Log Server | 1564

Junos OS supports configuring and monitoring of system log messages (also called *syslog messages*). You can configure files to log system messages and also assign attributes, such as severity levels, to messages. Reboot requests are recorded to the system log files, which you can view with the **show log** command.

This section contains the following topics:

Control Plane and Data Plane Logs

Junos OS generates separate log messages to record events that occur on the system's control and data planes.

- The control plane logs, also called system logs, include events that occur on the routing platform. The system sends control plane events to the **eventd** process on the Routing Engine, which then handles the events by using Junos OS policies, by generating system log messages, or both. You can choose to send control plane logs to a file, user terminal, routing platform console, or remote machine. To generate control plane logs, use the **syslog** statement at the **[system]** hierarchy level.
- The data plane logs, also called *security logs*, primarily include security events that are handled inside the data plane. Security logs can be in text or binary format, and they can be saved locally (event mode) or sent to an external server (stream mode). Binary format is required for stream mode and recommended to conserve log space in event mode.

  Note the following:

  - Security logs can be saved locally (on box) or externally (off box), but not both.
  - SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices default to stream mode. To specify binary format and an external server, see "Configuring Off-Box Binary Security Log Files" on page 1584.

    > **NOTE:** Logs might be dropped if you configure event mode logging on these devices.

    Starting with Junos OS Release 15.1X49-D100, the default mode for SRX1500 device is stream mode. Prior to Junos OS Release 15.1X49-D100, the default mode for SRX1500 device was event mode.
  - Starting in Junos OS Release 19.3R1, SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M devices default to stream mode. Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see "Configuring Off-Box Binary Security Log Files" on page 1584.

  Starting in Junos OS Release 20.2R1, we support escape in stream log forwarding and on-box reporting to avoid parsing errors. Stream mode supports escape in **sd-syslog** and **binary** formats when logs are not sent to **eventd** process. For the logs send to **eventd** process, we recommend not to enable an **escape** option as the **eventd** process has enabled the escape for the structure log. Event mode supports escape only in **binary** format. By default the **escape** option is disabled. You must enable the **escape** option using the **set security log escape** command.

Redundant System Log Server

Security system logging traffic intended for remote servers is sent through the network interface ports, which support two simultaneous system log destinations. Each system logging destination must be

configured separately. When two system log destination addresses are configured, identical logs are sent to both destinations. While two destinations can be configured on any device that supports the feature, adding a second destination is primarily useful as a redundant backup for standalone and active/backup configured chassis cluster deployments.

The following redundant server information is available:

- Facility: **cron**
- Description: cron scheduling process
- Severity Level (from highest to lowest severity): **debug**
- Description: Software debugging messages

Release History Table

Release	Description
15.1X49-D100	Starting with Junos OS Release 15.1X49-D100, the default mode for SRX1500 device is stream mode. Prior to Junos OS Release 15.1X49-D100, the default mode for SRX1500 device was event mode.
Junos OS Release 19.3R1	Starting in Junos OS Release 19.3R1, SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M devices default to stream mode.

Understanding Stream Logging for Security Devices

Junos OS supports forwarding logs using stream mode and event mode. All the categories can be configured for sending specific category logs to different log servers for stream mode log forwarding.

Stream mode log forwarding includes the following steps:

- An RTLOG system log message is generated by the data plane and is sent out from the Packet Forwarding Engine.
- An RTLOG system log message is generated by pfe process and is sent from Packet Forwarding Engine.
- An RTLOG system log message is generated by the Routing Engine unified threat management (utmd) process and is sent by rtlogd process from the Routing Engine.

For stream mode log forwarding, the transport protocol used between Packet Forwarding Engine and the log server can be UDP, TCP, or TLS. These transport protocols UDP, TCP, and TLS are configurable. The transport protocol used between the Routing Engine and the log server can only be UDP. TLS is not supported on cSRX.

Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts.
In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

Starting in Junos OS Release 20.2R1, we support escape in stream log forwarding to avoid parsing errors. Stream mode supports escape in **sd-syslog** and **binary** formats when logs are not sent to **eventd** process. For the logs send to **eventd** process, we recommend not to enable an **escape** option as the **eventd** process has enabled the escape for the structure log. By default the **escape** option is disabled. You must enable the **escape** option using the **set security log escape** command.

Release History Table

Release	Description
17.4R2	Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts. In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

RELATED DOCUMENTATION

- log (Security) | **2469**
- Understanding Binary Format for Security Logs | **1566**
- Setting the System to Send All Log Messages Through eventd | **1586**
- Setting the System to Stream Security Logs | **1587**
- Sending System Log Messages to a File | **1586**
- *Monitoring System Log Messages with the J-Web Event Viewer*

Understanding Binary Format for Security Logs

The Junos OS generates separate log messages to record events that occur on the system's control plane and data plane. The control plane monitors events that occur on the routing platform. Such events are recorded in system log messages. To generate system log messages, use the **syslog** statement at the **[system]** hierarchy level.

Data plane log messages, referred to as security log messages, record security events that the system handles directly inside the data plane. To generate security log messages, use the **log** statement at the **[security]** hierarchy level.

System log messages are maintained in log files in text-based formats, such as BSD Syslog, Structured Syslog, and WebTrends Enhanced Log Format (WELF).

Security log messages can also be maintained in text-based formats. Because security logging can produce large amounts of data, however, text-based log files can quickly consume storage and CPU resources. Depending on your implementation of security logging, a log file in a binary-based format can provide more efficient use of on-box or off-box storage and improved CPU utilization. Binary format for security log messages is available on all SRX Series devices.

When configured in event mode, security log messages generated in the data plane are directed to the control plane and stored locally on the device. Security log messages stored in binary format are maintained in a log file separate from that used to maintain system log messages. Events stored in a binary log file are not accessible with advanced log-scripting commands intended for text-based log files. A separate CLI operational command supports decoding, converting, and viewing binary log files that are stored locally on the device.

When configured in stream mode, security log messages generated in the data plane are streamed to a remote device. When these messages are stored in binary format, they are streamed directly to an external log collection server in a Juniper-specific binary format. Externally-stored binary log files can only be read using Juniper Secure Analytics (JSA) or Security Threat Response Manager (STRM).

Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts.
In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

For information about configuring on-box (event-mode) binary security logs, please see “Configuring On-Box Binary Security Log Files” on page 1582. For information about configuring off-box (stream-mode) binary security logs, please see “Configuring Off-Box Binary Security Log Files” on page 1584.

Release History Table

Release	Description
17.4R2	Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts. In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

RELATED DOCUMENTATION

Understanding System Logging for Security Devices | 1563

Understanding On-Box Logging and Reporting

This topic describes the on-box logging and reporting CLI functionality and the design aspects of on-box reporting for the SRX devices.

Overview

On-box traffic logging to solid-state drives (SSDs) supports eight external log servers or files.

An all-in-one XML file is added that contains all the traffic logs information. The XML file also generates all the logging header files and traffic log related documents.

A new process (daemon) called *local log management daemon (llmd)* is supported in Services Processing Cards 0 (SPCs0) to handle on-box traffic logging. Traffic produced by flowd in SPCs is listed in traffics logs. The llmd saves these logs to the local SSD. Traffic logs are saved in the following four different formats:

- syslog
- sd-syslog
- welf
- binary

On-box reporting mechanism is an enhancement to the existing logging functionality. The existing logging functionality is modified to collect system traffic logs, analyzes the logs, and generate reports of these logs in the form of tables using the CLI. On-box reporting feature is intended to provide a simple and easy to use interface for viewing security logs. The on-box reports are easy to use J-Web pages of various security events in the form of tables and graphs. The reports allow the IT security management to identify security information at a glance, and quickly decide the actions to be taken.

The on-box reporting feature is enabled by default when you load the factory-default configurations on the SRX Series device with Junos OS Release 15.1X49-D100 or later.

If you are upgrading your SRX Series device from a Junos OS Release prior to Junos OS 15.1X49-D100, then the SRX device inherits the existing configuration and the on-box reporting feature is disabled by default. You need to configure the **set security log report** command and the **set security log mode stream** command to enable the on-box reporting feature on the device that are upgraded.

Starting in Junos OS Release 19.3R1 , the factory-default configuration does not include on-box reporting configuration to increase the solid-state drive (SSD) lifetime. You can enable the on-box reporting feature by configuring the **set security log report** CLI command at **[edit security log]** hierarchy.

> **NOTE:** You must configure security policy for the session using the **set security policies from-zone zone-name to-zone zone-name policy *policy-name* then log session-close** command to list all the applications and nested applications in Application Tracking on J-Web using the on-box reporting feature. See for more *log (Security Policies)* for details.

After the log message is recorded, the log is stored within a log file which is then stored in the database table of the RE for further analysis (on SRX300, SRX320, SRX340, SRX345, and SRX550M devices) or on the SSD card for further analysis (on SRX1500, SRX4100, and SRX4200 devices).

> **NOTE:** This feature supports receiving top most reports based on count or volume of the session or the type of log, captures events occurring in each second within a specified time range, captures log content for a specified CLI condition. Various CLI conditions like “summary”, top”, “in-detail”, and “in-interval” are used to generate reports. You can generate only one report at one time using the CLI. All the CLI conditions cannot be used at the same time. You can generate only one report at one time using the CLI.

The benefits of this feature are:

- Reports are stored locally on the SRX Series device and there is no requirement for separate devices or tools for logs and reports storage.
- The on-box reports are easy-to-use J-Web pages of various security events in the form of tables and graphs.
- Provides a simple and easy-to-use interface for viewing security logs.
- The reports generated enables the IT security management team to identify security information at a glance and quickly decide the actions to be taken.

The on-box reporting feature supports:

- Generating reports based on the requirements. For example: count or volume of the session, types of logs for activities such as IDP, UTM, IPsec VPN.
- Capturing real-time events within a specified time range.
- Capturing all the network activities in a logical, organized, and easy-to-understand format based on various CLI specified conditions.

Understanding On-box Logging and Reporting

In the on-box reporting mechanism, CLI is used to fetch the reporting data from the device. The SRX series device collects and saves all the required logs. These recorded logs are then used for further analysis to

calculate and generate reports in the form of tables using the CLI. The data generated using CLI in the form of reports can be further retrieved in the form of tables and graphs in J-Web. The reports generated are easy-to-understand tables and graphs in J-Web. Thorough analysis of logs is performed (based on session types) for features such as screen, IDP, UTM and IPSec.

You can define filters for the log data that is reported on based on the following criteria:

> **NOTE:** The top, in-detail, and in-interval conditions cannot be used at the same time.

- **top *<number>***—This option allow you to generate reports for top security events as specified in the command. for example: top 5 IPS attacks or top 6 URLs detected through UTM.
- **in-detail *<number>***—This option allow you to generate detail log content.
- **in-interval *<time-period>***—This option allows you to generate the events logged between certain time intervals.
- **summary**—This option allows you to generate the summary of the events. In this way, you can fine-tune the report to your needs, and displays only the data that you want to use.

The maximum in-interval number which shows the count in intervals is 30. If large duration is specified, then the counters are assembled to ensure the maximum in-interval is less than 30.

Both in-detail and summary have the “all” option, since different table have different attribute (like session table does not have the attribute “reason” but UTM has), the “all” option does not have any filter except start-time and stop-time. If there is any other filter other than start time and stop time then an error is displayed.

For example: root@kujang> show security log report in-detail all reason reason1

```
error: "query condition error"
```

The application firewall logs for application and user visibility will list applications and nested applications. When the logs of these features list nested applications then nested applications are listed in J-Web. When the logs list nested applications as not-applicable or unknown then only the applications are listed in J-Web.

Use the following CLI commands for application and user visibility for all the applications and nested applications listing:

- For top nested-application by count—**show security log report top session-close top-number <number> group-by application order-by count with user**
- For top nested-application by volume—**show security log report top session-close top-number <number> group-by application order-by volume with user**

- For top user by count with nested application—**show security log report top session-close top-number <number> group-by user order-by count with application**

On-Box Reporting Features

The on-box reporting feature supports:

- **Sqlite3 support as a library**—sqlite3 was not supported prior to Junos OS release 15.1X49-D100. Starting with Junos OS Release 15.1X49-D100, an SQL log database (SQLite Version 3) is used by the daemons running on the RE as well as other potential modules to store logs on SRX Series devices.

  In Junos OS Release 19.4R1, we've upgraded the on-box logging database to improve query performance.

- **Running llmd in both Junos OS and Linux OS**—The forwarding daemon (flowd) decodes database index from binary logs and sends both index and log to the local log management daemon (llmd).

  On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, llmd runs in Junos OS. On SRX1500, SRX4100, and SRX4200 devices, llmd runs in Linux. So, for supporting llmd to run in both Junos OS and Linux OS, the llmd code directory is moved from the Linux side to the Junos OS side.

- **Storing of logs into specified table of the sqlite3 database by llmd**— A new syslog daemon is introduced to collect local logs on SRX Series devices and saving them into the database.

  Starting in Junos OS Release 19.3R1, Junos OS stores logs in multiple tables instead of a single table in a database file. Each table contains the timestamp of the oldest and latest logs. When you initiate a query based on the start and end time, llmd finds latest table to generate reports.

  For example, if there are 5 million logs in one table of a database file generated in the last 10 hours, and if you want to take a report, you should spend more than half an hour. From Junos OS Release 19.3R1, one table is separated into multiple tables, and each table has 0.5 million of logs. To generate the same report, one table information is sufficient.

  We recommend you to query with a shorter time for better performance.

  - **Database table definition**—For session logs, the data types are source-address, destination-address, application, user, and so on. For logs related to security features, the data types are attack-name, URL, profile protocol, and so on. Therefore, different tables are designed to store different types of logs to help improve the performance and save disk space. SRX device creates a database table for each log type, when log data is recorded.

    Each type of database table has its maximum record number that is device specific. When the table record number reaches the limitation, new logs replace the oldest logs. Junos OS stores log in an SRX Series device in which active traffic is passed.

    Starting in Junos OS Release 19.3R1, you can create multiple tables in a database file to store logs. You can define the capacity to store logs in a table.

    If the limit of log number exceeds the table capacity, Junos OS stores the logs in the second table. For example, if the limit of logs in table 1 exceeds the table capacity, Junos OS stores logs in table 2.

If the limit of the log number exceeds the last table of file 1, Junos OS stores the logs in table 1 of file 2. For example, table n is the last table of file 1. When the logs exceed the table capacity, Junos OS stores the logs in table 1 of file 2.

To make immediate effect after you change the table number, use **clear security log report** operational command.

- **Database table rotation**—Each type of database table has its maximum record number that is device specific. When the table record number reaches the limitation, new logs replace the oldest logs.

  Following Table 174 on page 1572 describes the database file size capacity:

  Table 174: Database File Size Capacity

Devices	Session	Screen	IDP	UTM	IPsec-VPN	SKY
SRX300, SRX320, SRX340, SRX345, and SRX550M	1.8G	0.18G	0.18G	0.18G	0.06G	0.18G
SRX1500	12G	2.25G	2.25G	2.25G	0.75G	2.25G
SRX4100 and SRX4200	15G	2.25G	2.25G	2.25G	0.75G	2.25G
SRX4600	22.5G	6G	6G	6G	0.75G	2.25G
vSRX	1.8G	0.18G	0.18G	0.18G	0.06G	0.18G

- **Calculating and displaying the reports that are triggered by CLI**—The reports from the database are received from the CLI as the interface. Using the CLI, you can calculate and display the reporting details.

Table Selection

When you want to generate a report from multiple tables, llmd sorts tables based on timestamp and selects tables as per the requested start-time and stop-time.

For example, there are three tables that is table 1 (1 to 3), table 2 (3 to 5) and table 3 (6 to 8). 1 to 3, 3 to 6, and 6 to 8 denotes time stamp of latest and oldest logs. If you request a report from 4 to 6, Junos OS generates report from table 2 and table 3.

Table Lifetime

You can decide table lifetime by configuring **set security log report table-lifetime** command. Junos OS removes the table after the table identify time exceeds the table lifetime. For example, if you configure table lifetime as 2, and the current date is 26-July-2019, then it means on 24-July-2019 00:00:00 logs are removed.

If you change the date and time manually on a device, the table lifetime changes. For example, if a table identify time is 19-July-2019, and you configure table lifetime as 10, Junos OS should remove the table on 29-July-2019. If you change the device date as 18-July-2019, then the table real lifetime becomes 30-July-2019.

Table Dense Mode

In Junos OS Release 19.4R1, we've upgraded the default storage and search mechanism in the on-box logging database to manage logs. You can now customize log storage and search mechanism results. For example, if you expect fewer traffic logs, you can use the default configuration with a start time and a stop time.

However, if you expect a large number of traffic logs and greater time intervals for which the logs will be generated, then enable dense mode. To enable dense mode, use the **set security log report table-mode dense** configuration command.

Chassis Cluster Scenario

For on-box reporting in a chassis cluster, the logs are stored in the local disk on which the device is processing active traffic. These logs are not synchronized to the chassis cluster peer.

Each node is responsible to store logs when each node is processing active traffic. In case of active/passive mode, only the active node processes the traffic and logs are also stored only in the active node. In case of failover, the new active node is processes the traffic and stores logs in its local disk. In case of active/active mode, each node processes its own traffic and logs are stored in the respective nodes.

Release History Table

Release	Description
Junos OS Release 15.1X49-D100	The on-box reporting feature is enabled by default when you load the factory-default configurations on the SRX Series device with Junos OS Release 15.1X49-D100 or later.
Junos OS Release 19.3R1	Starting in Junos OS Release 19.3R1 , the factory-default configuration does not include on-box reporting configuration to increase the solid-state drive (SSD) lifetime.

RELATED DOCUMENTATION

report | **2498**

Example: Configuring Application Tracking

Monitoring Reports

IN THIS SECTION

- Threats Monitoring Report | 1574
- Traffic Monitoring Report | 1580

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action. The J-Web reporting feature provides one- or two-page reports that are equivalent to a compilation of numerous log entries.

This section contains the following topics:

Threats Monitoring Report

Purpose

Use the Threats Report to monitor general statistics and activity reports of current threats to the network. You can analyze logging data for threat type, source and destination details, and threat frequency information. The report calculates, displays, and refreshes the statistics, providing graphic presentations of the current state of the network.

Action

To view the Threats Report:

1. Click **Threats Report** in the bottom right of the Dashboard, or select **Monitor>Reports>Threats** in the J-Web user interface. The Threats Report appears.

2. Select one of the following tabs:
   - **Statistics** tab. See Table 124 on page 1111 for a description of the page content.
   - **Activities** tab. See Table 125 on page 1113 for a description of the page content.

Table 175: Statistics Tab Output in the Threats Report

Field	Description
General Statistics Pane	

Table 175: Statistics Tab Output in the Threats Report *(continued)*

Field	Description

Threat Category	One of the following categories of threats:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter—Click the Web filter category to display counters for 39 subcategories.
	  ◦ Content Filter
	• Firewall Event

Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Hits in past 24 hours	Number of threats encountered per category in the past 24 hours.
Hits in current hour	Number of threats encountered per category in the last hour.
Threat Counts in the Past 24 Hours	
By Severity	Graph representing the number of threats received each hour for the past 24 hours sorted by severity level.
By Category	Graph representing the number of threats received each hour for the past 24 hours sorted by category.
X Axis	Twenty-four hour span with the current hour occupying the right-most column of the display. The graph shifts to the left every hour.
Y Axis	Number of threats encountered. The axis automatically scales based on the number of threats encountered.

Table 175: Statistics Tab Output in the Threats Report *(continued)*

Field	Description
Most Recent Threats	
Threat Name	Names of the most recent threats. Depending on the threat category, you can click the threat name to go to a scan engine site for a threat description.

Category	Category of each threat:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter
	  ◦ Content Filter
	• Firewall Event

Source IP/Port	Source IP address (and port number, if applicable) of the threat.
Destination IP/Port	Destination IP address (and port number, if applicable) of the threat.
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail
Action	Action taken in response to the threat.
Hit Time	Time the threat occurred.
Threat Trend in past 24 hours	

Table 175: Statistics Tab Output in the Threats Report *(continued)*

Field	Description

Category	Pie chart graphic representing comparative threat counts by category:
	• Traffic
	• IDP
	• Content Security
	  ◦ Antivirus
	  ◦ Antispam
	  ◦ Web Filter
	  ◦ Content Filter
	• Firewall Event

Web Filter Counters Summary	
Category	Web filter count broken down by up to 39 subcategories. Clicking on the Web filter listing in the General Statistics pane opens the Web Filter Counters Summary pane.
Hits in past 24 hours	Number of threats per subcategory in the last 24 hours.
Hits in current hour	Number of threats per subcategory in the last hour.

Table 176: Activities Tab Output in the Threats Report

Field	Function
Most Recent Virus Hits	
Threat Name	Name of the virus threat. Viruses can be based on services, like Web, FTP, or e-mail, or based on severity level.
Severity	Severity level of each threat: • emerg • alert • crit • err • warning • notice • info • debug

Table 176: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Source IP/Port	IP address (and port number, if applicable) of the source of the threat.
Destination IP/Port	IP address (and port number, if applicable) of the destination of the threat.
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail
Action	Action taken in response to the threat.
Last Hit Time	Last time the threat occurred.
Most Recent Spam E-Mail Senders	
From e-mail	E-mail address that was the source of the spam.
Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP	IP address of the source of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time that the spam e-mail was sent.
Recently Blocked URL Requests	
URL	URL request that was blocked.

Table 176: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Hits in current hour	Number of threats encountered in the last hour.
Most Recent IDP Attacks	
Attack	
Severity	Severity of each threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Protocol	Protocol name of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time the IDP threat was sent.

SEE ALSO

Traffic Monitoring Report | 1116

Monitoring Address Pools

Traffic Monitoring Report

Purpose

Monitor network traffic by reviewing reports of flow sessions over the past 24 hours. You can analyze logging data for connection statistics and session usage by a transport protocol.

Action

To view network traffic in the past 24 hours, select **Monitor>Reports>Traffic** in the J-Web user interface. See Table 126 on page 1117 for a description of the report.

Table 177: Traffic Report Output

Field	Description
Sessions in Past 24 Hours per Protocol	
Protocol Name	Name of the protocol. To see hourly activity by protocol, click the protocol name and review the “Protocol activities chart” in the lower pane. • TCP • UDP • ICMP
Total Session	Total number of sessions for the protocol in the past 24 hours.
Bytes In (KB)	Total number of incoming bytes in KB.
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Most Recently Closed Sessions	
Source IP/Port	Source IP address (and port number, if applicable) of the closed session.
Destination IP/Port	Destination IP address (and port number, if applicable) of the closed session.
Protocol	Protocol of the closed session. • TCP • UDP • ICMP
Bytes In (KB)	Total number of incoming bytes in KB.

Table 177: Traffic Report Output *(continued)*

Field	Description
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Timestamp	The time the session was closed.
Protocol Activities Chart	
Bytes In/Out	Graphic representation of traffic as incoming and outgoing bytes per hour. The byte count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
Packets In/Out	Graphic representation of traffic as incoming and outgoing packets per hour. The packet count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
Sessions	Graphic representation of traffic as the number of sessions per hour. The session count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
X Axis	One hour per column for 24 hours.
Y Axis	Byte, packet, or session count.
Protocol Session Chart	
Sessions by Protocol	Graphic representation of the traffic as the current session count per protocol. The protocols displayed are TCP, UDP, and ICMP.

SEE ALSO

Threats Monitoring Report | 1110

RELATED DOCUMENTATION

Monitoring Overview | 15

Configuring On-Box Binary Security Log Files

SRX Series devices use two types of logs—system logs and security logs—to record system events. System logs record control plane events—for example, when an admin user logs in. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling. For example, Junos OS generates a security log if a security policy denies certain traffic because of a policy violation. For more about system logs, see "Junos OS System Log Overview" on page 1467. For more information about security logs, see "Understanding System Logging for Security Devices" on page 1563.

You can collect and save both system and security logs in binary format either on-box (that is, stored locally on the SRX Series device) or off-box (streamed to a remote device). Using binary format ensures that log files are efficiently stored, which in turn improves CPU utilization.

You can configure security files in binary format using the **log** statement at the **[security]** hierarchy level.

On-box logging is also known as event-mode logging. For stream-mode, off-box security logging, see "Configuring Off-Box Binary Security Log Files" on page 1584. When you configure security logs in binary format for event-mode logging, you can optionally define the log filename, file path, and other characteristics, as detailed in the following procedure:

1. Specify the logging mode and format for on-box logging::

```
[edit security]
user@host# set log mode event
user@host# set log format binary
```

> **NOTE:** If you configure system logging to send system logs to an external destination (that is, off-box or stream-mode), security logs are also sent to that destination even if you are using event-mode security logging. For more information about sending system logs to an external destination, see "Examples: Configuring System Logging" on page 1502.

> **NOTE:** Off-box and on-box security logging modes cannot be enabled simultaneously.

2. (Optional) Define a name and path for the log file.

NOTE: By default, the bin_messages file is created in the /var/log directory.

```
[edit security]
user@host# set log file name security-binary-log
user@host# set log file path security/log-folder
```

3. (Optional) Change the maximum size of the log file and the maximum number of log files that can be archived.

   NOTE: By default, the maximum size of the log file is 3 MB, and a total of three log files can be archived.

   In the following sample commands, you set a value of 5 MB and 5 archived files, respectively:

```
[edit security]
user@host# set log file size 5
user@host# set log file files 5
```

4. (Optional) Configure the hpl flag to enable diagnostic traces for the binary security log files. The smf_hpl prefix identifies all binary logging traces.

```
[edit security]
user@host# set log traceoptions flag hpl
```

5. For the default-permit security policy, traffic logs for **RT_FLOW** are generated when a session ends.

```
[edit security]
user@host# set policies from-zone trust to-zone untrust policy default-permit then log session-close
```

6. (Optional) Traffic logs for **RT_FlOW** are generated when a session starts.

```
[edit security]
user@host# set policies from-zone trust to-zone untrust policy default-permit then log session-init
```

View the content of the event-mode log file stored on the device using **show security log file** command and use **clear security log file** command to clear the content of the binary event-mode security log file.

> **NOTE:** The **show security log** command displays event-mode security log messages if they are in a text-based format and the **show security log file** command displays event-mode security log messages if they are in binary format (on-box). Off-box binary logging is read by Juniper Secure Analytics (JSA).

RELATED DOCUMENTATION

Understanding Binary Format for Security Logs | **1566**

Setting the System to Send All Log Messages Through eventd | **1586**

Configuring Off-Box Binary Security Log Files

SRX Series devices have two types of log: system logs and security logs. System logs record control plane events, for example admin login to the device. For more about system logs, please see "Junos OS System Log Overview" on page 1467. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy. For more information about security logs, please see "Understanding System Logging for Security Devices" on page 1563.

The two types of log can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

You can configure security files in binary format using the **log** statement at the **[security]** hierarchy level.

The following procedure specifies binary format for stream-mode security logging, and defines the log filename, path, and log file characteristics. For event-mode, on-box security logging, please see "Configuring On-Box Binary Security Log Files" on page 1582.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging:

```
set security log mode stream
set security log stream test-stream format binary host 1.3.54.22
```

NOTE: Off-box and on-box security logging modes cannot be enabled simultaneously.

2. For off-box security logging, specify the source address, which identifies the SRX Series device that generated the log messages. The source address is required.

```
set security log source-address 2.3.45.66
```

3. Optionally, define a log filename and a path. By default, the file bin_messages is created in the /var/log directory.

```
set security log file name security-binary-log
set security log file path security/log-folder
```

4. Optionally, change the maximum size of the log file and the maximum number of log files that can be archived. By default the maximum size of the log file is 3 MB, and a total of three log files can be archived.

```
set security log file size 5
set security log file files 5
```

5. Optionally, select the hpl flag to enable diagnostic traces for binary logging. The prefix smf_hpl identifies all binary logging traces.

```
set security log traceoptions flag hpl
```

6. View the content of the event-mode log file stored on the device using either Juniper Secure Analytics (JSA) or Security Threat Response Manager (STRM).

RELATED DOCUMENTATION

Understanding Binary Format for Security Logs | 1566

Setting the System to Send All Log Messages Through eventd | 1586

Setting the System to Stream Security Logs | 1587

Sending System Log Messages to a File

You can direct system log messages to a file on the CompactFlash (CF) card. The default directory for log files is **/var/log**. To specify a different directory on the CF card, include the complete pathname.

Create a file named **security**, and send log messages of the **authorization** class at the severity level **info** to the file.

To set the filename, the facility, and severity level:

```
{primary:node0}
user@host# set system syslog file security authorization info
```

RELATED DOCUMENTATION

Understanding System Logging for Security Devices | 1563

Understanding Binary Format for Security Logs | 1566

Setting the System to Send All Log Messages Through eventd | 1586

Setting the System to Stream Security Logs | 1587

Monitoring System Log Messages with the J-Web Event Viewer

Setting the System to Send All Log Messages Through eventd

The **eventd** process of logging configuration is most commonly used for Junos OS. In this configuration, control plane logs and data plane, or security, logs are forwarded from the data plane to the Routing Engine control plane **rtlogd** process. The **rtlogd** process then either forwards syslog or sd-syslog-formatted logs to the **eventd** process or the WELF-formatted logs to the external or remote WELF log collector.

To send all log messages through **eventd**:

1. Set the **eventd** process to handle security logs and send them to a remote server.

   ```
   {primary:node0}
   user@host# set security log mode event
   ```

2. Configure the server that will receive the system log messages.

```
{primary:node0}
user@host# set system syslog host hostname any any
```

where ***hostname*** is the fully qualified hostname or IP address of the server that will receive the logs.

NOTE: To send duplicate logs to a second remote server, repeat the command with a new fully qualified *hostname* or IP address of a second server.

If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

To rename or redirect one of the logging configurations, you need to delete and recreate it. To delete a configuration:

```
{primary:node0}
user@host# delete security log mode event
```

RELATED DOCUMENTATION

Understanding System Logging for Security Devices | 1563

Understanding Binary Format for Security Logs | 1566

Setting the System to Stream Security Logs | 1587

Sending System Log Messages to a File | 1586

Monitoring System Log Messages with the J-Web Event Viewer

Setting the System to Stream Security Logs

You can increase the number of data plane, or security, logs that are sent by modifying the manner in which they are sent. When the logging mode is set to **stream**, security logs generated in the data plane are streamed out a revenue traffic port directly to a remote server.

NOTE: If the route of the remote server exists in the forwarding table, then the logs are forwarded to next hop points, irrespective of a physical interface or a logical interface.

To use the **stream** mode, enter the following commands:

```
{primary:node0}
user@host# set security log source-address source-address
user@host# set security log stream streamname format (syslog|sd-syslog|welf) category (all|content-security)
   host ipaddr
```

where *source-address* is the IP address of the source machine; **syslog**, **sd-syslog** (structured system logging messages) and **welf** are logging formats; **all** and **content-security** are the categories of logging; and *ipaddr* is the IP address of the server to which the logs will be streamed.

NOTE: WELF logs must be streamed through a revenue port because the **eventd** process does not recognize the WELF format. The category must be set to **content-security**. For example:

```
{primary:node0}
user@host# set security log stream securitylog1 format
   welf category content-security host 10.121.23.5
```

To send duplicate logs to a second remote server, repeat the command with a new *ipaddr*. If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

When a connection to a server is unreachable, SRX Series device tries to restore the connection, and Junos OS saves the log in the buffer during this period.

Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, use the **set security log stream *stream_name*** command to configure the stream log file.On SRX300, SRX320, SRX340, and SRX345 Series devices, use the **set security log stream *stream_name* host *host_IP address*** command to configure the stream log file with the source address and source interface attributes configuration.

Example:

```
[edit]
user@host# set security log mode stream
user@host# set security log source-address 192.0.2.1
user@host# set security log stream S1 host 192.0.2.2
user@host# set security log stream S1 format syslog
user@host# set security log stream S1 category all
user@host# set security log stream S2 file name file1
```

You can use the **show security log** command to verify the log configuration.

The following sample output provides the log configuration:

user@host# show security log

```
mode stream;
source-address 192.0.2.1;
stream S1 {
    format syslog;
    category all;
    host {
        192.0.2.2;
    }
}
stream S2 {
    file {
        name file1;
    }
}
```

Starting from Junos OS Release 15.1X49-D120 and Junos OS Release 18.1R1 the maximum length of the syslog message in stream mode is increased from 1024 bytes to 1340 bytes.

Starting in Junos OS Release 20.2R1, the maximum length of the stream mode **sd-syslog** format syslog message is 4*1472 bytes.

Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts.
In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

Release History Table

Release	Description
17.4R2	Starting in Junos OS Release 17.4R2 and later, on SRX300, SRX320, SRX340, SRX345 Series devices and vSRX instances, when the device is configured in stream mode, you can configure maximum of eight system log hosts. In Junos OS Release 17.4R2 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.
15.1X49-D70	Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, use the **set security log stream *stream_name*** command to configure the stream log file.On SRX300, SRX320, SRX340, and SRX345 Series devices, use the **set security log stream *stream_name* host *host_IP address*** command to configure the stream log file with the source address and source interface attributes configuration.
15.1X49-D120	Starting from Junos OS Release 15.1X49-D120 and Junos OS Release 18.1R1 the maximum length of the syslog message in stream mode is increased from 1024 bytes to 1340 bytes.

RELATED DOCUMENTATION

- Understanding System Logging for Security Devices | **1563**
- Understanding Binary Format for Security Logs | **1566**
- Setting the System to Send All Log Messages Through eventd | **1586**
- Sending System Log Messages to a File | **1586**
- *Monitoring System Log Messages with the J-Web Event Viewer*
- *Configuring the TLS Syslog Protocol on SRX Series device*

CHAPTER 52

Monitoring Log Messages

IN THIS CHAPTER

- Monitoring System Log Messages | 1591

Monitoring System Log Messages

Purpose

Display system log messages about the QFX Series. By looking through a system log file for any entries pertaining to the interface that you are interested in, you can further investigate a problem with an interface on the switch.

Action

To view system log messages:

```
user@switch1> show log messages
```

Sample Output

```
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 1
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 2
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 3
...
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Management process): new instance detected (variable:
sysApplElmtRunMemory.5.6.2293)
```

```
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Command-line interface): new instance detected (variable:
sysApplElmtRunMemory.5.8.2292)
...
Nov  4 12:10:24  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'exit '
Nov  4 12:10:27  switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
configuration mode
Nov  4 12:10:31  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'show log messages
```

Meaning

The sample output shows the following entries in the **messages** file:

- A new log file was created when the previous file reached the maximum size of 128 kilobytes (KB).
- The fan speed for Fan 1, 2, and 3 is set at 65 percent.
- Health monitoring activity is detected.
- CLI commands were entered by the user jsmith.

RELATED DOCUMENTATION

Overview of Junos OS System Log Messages | **1468**

Understanding the Implementation of System Log Messages on the QFabric System

Example: Configuring System Log Messages | **1487**

clear log | **2920**

show log | **2936**

syslog | **2510**

PART 12

Network Management and Troubleshooting

Monitoring and Troubleshooting | **1594**

Troubleshooting of System Performance with Resource Monitoring Methodology | **1616**

Configuring Data Path Debugging and Trace Options | **1627**

Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits | **1646**

Using Packet Capture to Analyze Network Traffic | **1659**

Troubleshooting Security Devices | **1687**

CHAPTER 53

Monitoring and Troubleshooting

IN THIS CHAPTER

- Pinging Hosts | 1594
- Monitoring Traffic Through the Router or Switch | 1595
- Dynamic Ternary Content Addressable Memory Overview | 1599
- Service Scaling on ACX5048 and ACX5096 Routers | 1611
- Understanding and Configuring the Unified Forwarding Table | 1611
- Troubleshooting and Monitoring TCAM Resource in ACX Series Routers | 1614

Pinging Hosts

Purpose

Use the CLI **ping** command to verify that a host can be reached over the network. This command is useful for diagnosing host and network connectivity problems. The switch sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to a specified host and receives ICMP echo responses.

Action

To use the **ping** command to send four requests (ping count) to host3:

ping *host* count *number*

Sample Output

ping host3 count 4

```
user@switch> ping host3 count 4
PING host3.site.net (192.0.2.111): 56 data bytes
64 bytes from 192.0.2.111: icmp_seq=0 ttl=122 time=0.661 ms
64 bytes from 192.0.2.111: icmp_seq=1 ttl=122 time=0.619 ms
64 bytes from 192.0.2.111: icmp_seq=2 ttl=122 time=0.621 ms
```

```
64 bytes from 192.0.2.111: icmp_seq=3 ttl=122 time=0.634 ms

--- host3.site.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

Meaning

- The **ping** results show the following information:
  - Size of the ping response packet (in bytes).
  - IP address of the host from which the response was sent.
  - Sequence number of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
  - Time-to-live (ttl) hop-count value of the ping response packet.
  - Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
  - Number of ping requests (probes) sent to the host.
  - Number of ping responses received from the host.
  - Packet loss percentage.
  - Round-trip time statistics: minimum, average, maximum, and standard deviation of the round-trip time.

RELATED DOCUMENTATION

> *Troubleshooting Overview*
>
> *Understanding Troubleshooting Resources*

Monitoring Traffic Through the Router or Switch

To help with the diagnosis of a problem, display real-time statistics about the traffic passing through physical interfaces on the router or switch.

To display real-time statistics about physical interfaces, perform these tasks:

1. Displaying Real-Time Statistics About All Interfaces on the Router or Switch | **1596**
2. Displaying Real-Time Statistics About an Interface on the Router or Switch | **1597**

Displaying Real-Time Statistics About All Interfaces on the Router or Switch

Purpose

Display real-time statistics about traffic passing through all interfaces on the router or switch.

Action

To display real-time statistics about traffic passing through all interfaces on the router or switch:

```
user@host> monitor interface traffic
```

Sample Output

`user@host>` **monitor interface traffic**

```
host name                  Seconds: 15                  Time: 12:31:09
Interface    Link  Input packets        (pps)     Output packets        (pps)
 so-1/0/0    Down              0          (0)                  0          (0)
 so-1/1/0    Down              0          (0)                  0          (0)
 so-1/1/1    Down              0          (0)                  0          (0)
 so-1/1/2    Down              0          (0)                  0          (0)
 so-1/1/3    Down              0          (0)                  0          (0)
 t3-1/2/0    Down              0          (0)                  0          (0)
 t3-1/2/1    Down              0          (0)                  0          (0)
 t3-1/2/2    Down              0          (0)                  0          (0)
 t3-1/2/3    Down              0          (0)                  0          (0)
 so-2/0/0      Up         211035           (1)              36778          (0)
 so-2/0/1      Up         192753          (1)              36782          (0)
 so-2/0/2      Up         211020          (1)              36779          (0)
 so-2/0/3      Up         211029          (1)              36776          (0)
 so-2/1/0      Up         189378          (1)              36349          (0)
 so-2/1/1    Down              0          (0)              18747          (0)
 so-2/1/2    Down              0          (0)              16078          (0)
 so-2/1/3      Up              0          (0)              80338          (0)
 at-2/3/0      Up              0          (0)                  0          (0)
 at-2/3/1    Down              0          (0)                  0          (0)
Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D
```

Meaning

The sample output displays traffic data for active interfaces and the amount that each field has changed since the command started or since the counters were cleared by using the **C** key. In this example, the

monitor interface command has been running for 15 seconds since the command was issued or since the counters last returned to zero.

Displaying Real-Time Statistics About an Interface on the Router or Switch

Purpose

Display real-time statistics about traffic passing through an interface on the router or switch.

Action

To display traffic passing through an interface on the router or switch, use the following Junos OS CLI operational mode command:

```
user@host> monitor interface interface-name
```

Sample Output

`user@host>` **monitor interface so-0/0/1**

```
Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
R1
Interface: so-0/0/1, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC3 Traffic statistics:
  Input bytes:                   5856541 (88 bps)
  Output bytes:                  6271468 (96 bps)
  Input packets:                  157629 (0 pps)
  Output packets:                 157024 (0 pps)
Encapsulation statistics:
  Input keepalives:                42353
  Output keepalives:               42320
  LCP state: Opened
Error statistics:
  Input errors:                        0
  Input drops:                         0
  Input framing errors:                0
  Input runts:                         0
  Input giants:                        0
  Policed discards:                    0
  L3 incompletes:                      0
  L2 channel errors:                   0
  L2 mismatch timeouts:                0
  Carrier transitions:                 1
```

```
  Output errors:                          0
  Output drops:                           0
  Aged packets:                           0
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                               1
  LOF count                               1
  SEF count                               1
  ES-S                                   77
  SES-S                                  77
SONET statistics:
  BIP-B1                                  0
  BIP-B2                                  0
  REI-L                                   0
  BIP-B3                                  0
  REI-P                                   0
Received SONET overhead:  F1        : 0x00  J0        : 0xZ
```

Meaning

The sample output shows the input and output packets for a particular SONET interface (**so-0/0/1**). The information can include common interface failures, such as SONET/SDH and T3 alarms, loopbacks detected, and increases in framing errors. For more information, see *Checklist for Tracking Error Conditions*.

To control the output of the command while it is running, use the keys shown in Table 178 on page 1598.

Table 178: Output Control Keys for the monitor interface Command

Action	Key
Display information about the next interface. The **monitor interface** command scrolls through the physical or logical interfaces in the same order that they are displayed by the **show interfaces terse** command.	**N**
Display information about a different interface. The command prompts you for the name of a specific interface.	**I**
Freeze the display, halting the display of updated statistics.	**F**
Thaw the display, resuming the display of updated statistics.	**T**
Clear (zero) the current delta counters since **monitor interface** was started. It does not clear the accumulative counter.	**C**

Table 178: Output Control Keys for the monitor interface Command *(continued)*

Action	Key
Stop the **monitor interface** command.	**Q**

See the CLI Explorer for details on using match conditions with the **monitor traffic** command.

Dynamic Ternary Content Addressable Memory Overview

IN THIS SECTION

- Understanding Dynamic Ternary Content Addressable Memory | **1599**
- Applications using Dynamic TCAM Infrastructure | **1599**
- Features Using TCAM Resource | **1600**
- Monitoring TCAM Resource Usage | **1603**
- Example: Monitoring and Troubleshooting the TCAM Resource | **1604**

Understanding Dynamic Ternary Content Addressable Memory

In ACX Series routers, Ternary Content Addressable Memory (TCAM) is used by various applications like firewall, connectivity fault management, PTPoE, RFC 2544, etc. The Packet Forwarding Engine (PFE) in ACX Series routers uses TCAM with defined TCAM space limits. The allocation of TCAM resources for various filter applications are statically distributed. This static allocation leads to inefficient utilization of TCAM resources when all the filter applications might not use this TCAM resource simultaneously.

The dynamic allocation of TCAM space in ACX routers efficiently allocates the available TCAM resources for various filter applications. In the dynamic TCAM model, various filter applications (such as inet-firewall, bridge-firewall, cfm-filters, etc.) can optimally utilize the available TCAM resources as and when required. Dynamic TCAM resource allocation is usage driven and is dynamically allocated for filter applications on a need basis. When a filter application no longer uses the TCAM space, the resource is freed and available for use by other applications. This dynamic TCAM model caters to higher scale of TCAM resource utilization based on application's demand.

Applications using Dynamic TCAM Infrastructure

The following filter application categories use the dynamic TCAM infrastructure:

- Firewall filter—All the firewall configurations
- Implicit filter—Routing Engine (RE) demons using filters to achieve its functionality. For example, connectivity fault management, IP MAC validation, etc.
- Dynamic filters—Applications using filters to achieve the functionality at the PFE level. For example, logical interface level fixed classifier, RFC 2544, etc. RE demons will not know about these filters.
- System-init filters—Filters that require entries at the system level or fixed set of entries at router's boot sequence. For example, Layer 2 and Layer 3 control protocol trap, default ARP policer, etc.

> **NOTE:** The System-init filter which has the applications for Layer 2 and Layer 3 control protocols trap is essential for the overall system functionality. The applications in this control group consume a fixed and minimal TCAM space from the overall TCAM space. The system-init filter will not use the dynamic TCAM infrastructure and will be created when the router is initialized during the boot sequence.

Features Using TCAM Resource

Applications using the TCAM resource is termed tcam-app in this document. For example, inet-firewall, bridge-firewall, connectivity fault management, link fault management, etc., are all different tcam-apps.

Table 179 on page 1600 describes the list of tcam-apps that use TCAM resources.

Table 179: Features Using TCAM Resource

TCAM Apps/TCAM Users	Feature/Functionality	TCAM Stage
bd-dtag-validate	Bridge domain dual-tagged validate **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Egress
bd-tpid-swap	Bridge domain vlan-map with swap tpid operation	Egress
cfm-bd-filter	Connectivity fault management implicit bridge-domain filters	Ingress
cfm-filter	Connectivity fault management implicit filters	Ingress
cfm-vpls-filter	Connectivity fault management implicit vpls filters **NOTE:** This feature is supported only on ACX5048 and ACX5096 routers.	Ingress

Table 179: Features Using TCAM Resource *(continued)*

TCAM Apps/TCAM Users	Feature/Functionality	TCAM Stage
cfm-vpls-ifl-filter	Connectivity fault management implicit vpls logical interface filters **NOTE:** This feature is supported only on ACX5048 and ACX5096 routers.	Ingress
cos-fc	Logical interface level fixed classifier	Pre-ingress
fw-ccc-in	Circuit cross-connect family ingress firewall	Ingress
fw-family-out	Family level egress firewall	Egress
fw-fbf	Firewall filter-based forwarding	Pre-ingress
fw-fbf-inet6	Firewall filter-based forwarding for inet6 family	Pre-ingress
fw-ifl-in	Logical interface level ingress firewall	Ingress
fw-ifl-out	Logical interface level egress firewall	Egress
fw-inet-ftf	Inet family ingress firewall on a forwarding-table	Ingress
fw-inet6-ftf	Inet6 family ingress firewall on a forwarding-table	Ingress
fw-inet-in	Inet family ingress firewall	Ingress
fw-inet-rpf	Inet family ingress firewall on RPF fail check	Ingress
fw-inet6-in	Inet6 family ingress firewall	Ingress
fw-inet6-family-out	Inet6 Family level egress firewall	Egress
fw-inet6-rpf	Inet6 family ingress firewall on a RPF fail check	Ingress
fw-inet-pm	Inet family firewall with port-mirror action **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress
fw-l2-in	Bridge family ingress firewall on Layer 2 interface	Ingress
fw-mpls-in	MPLS family ingress firewall	Ingress

Table 179: Features Using TCAM Resource *(continued)*

TCAM Apps/TCAM Users	Feature/Functionality	TCAM Stage
fw-semantics	Firewall sharing semantics for CLI configured firewall	Pre-ingress
fw-vpls-in	VPLS family ingress firewall on VPLS interface	Ingress
ifd-src-mac-fil	Physical interface level source MAC filter	Pre-ingress
ifl-statistics-in	Logical level interface statistics at ingress	Ingress
ifl-statistics-out	Logical level interface statistics at egress	Egress
ing-out-iff	Ingress application on behalf of egress family filter for log and syslog	Ingress
ip-mac-val	IP MAC validation	Pre-ingress
ip-mac-val-bcast	IP MAC validation for broadcast	Pre-ingress
ipsec-reverse-fil	Reverse filters for IPsec service **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress
irb-cos-rw	IRB CoS rewrite	Egress
lfm-802.3ah-in	Link fault management (IEEE 802.3ah) at ingress **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress
lfm-802.3ah-out	Link fault management (IEEE 802.3ah) at egress	Egress
lo0-inet-fil	Looback interface inet filter	Ingress
lo0-inet6-fil	Looback interface inet6 filter	Ingress
mac-drop-cnt	Statistics for drops by MAC validate and source MAC filters	Ingress
mrouter-port-in	Multicast router port for snooping	Ingress

Table 179: Features Using TCAM Resource *(continued)*

TCAM Apps/TCAM Users	Feature/Functionality	TCAM Stage
napt-reverse-fil	Reverse filters for network address port translation (NAPT) service **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress
no-local-switching	Bridge no-local-switching	Ingress
ptpoe	Point-to-Point-Over-the-Ethernet traps **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress
ptpoe-cos-rw	CoS rewrite for PTPoE **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Egress
rfc2544-layer2-in	RFC2544 for Layer 2 service at ingress	Pre-ingress
rfc2544-layer2-out	RFC2544 for Layer 2 service at egress **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Egress
service-filter-in	Service filter at ingress **NOTE:** This feature is not supported on ACX5048 and ACX5096 routers.	Ingress

Monitoring TCAM Resource Usage

You can use the show and clear commands to monitor and troubleshoot dynamic TCAM resource usage.

Table 180 on page 1603 summarizes the command-line interface (CLI) commands you can use to monitor and troubleshoot dynamic TCAM resource usage.

Table 180: Show and Clear Commands to Monitor and Troubleshoot Dynamic TCAM

Task	Command
Display the shared and the related applications for a particular application	*show pfe tcam app*

Table 180: Show and Clear Commands to Monitor and Troubleshoot Dynamic TCAM *(continued)*

Task	Command
Display the TCAM resource usage for an application and stages (egress, ingress, and pre-ingress)	*show pfe tcam usage*
Display the TCAM resource usage errors for applications and stages (egress, ingress, and pre-ingress)	*show pfe tcam errors*
Clears the TCAM resource usage error statistics for applications and stages (egress, ingress, and pre-ingress)	*clear pfe tcam-errors*

Example: Monitoring and Troubleshooting the TCAM Resource

This section describes a use case where you can monitor and troubleshoot TCAM resources using show commands. In this use case scenario, you have configured Layer 2 services and the Layer 2 service-related applications are using TCAM resources. The dynamic approach, as shown in this example, gives you the complete flexibility to manage TCAM resources on a need basis.

The service requirement is as follows:

- Each bridge domain has one UNI and one NNI interface
- Each UNI interface has:
  - One logical interface level policer to police the traffic at 10 Mbps.
  - Multifield classifier with four terms to assign forwarding class and loss-priority.
- Each UNI interface configures CFM UP MEP at the level 4.
- Each NNI interface configures CFM DOWN MEP at the level 2

Let us consider a scenario where there are 100 services configured on the router. With this scale, all the applications are configured successfully and the status shows **OK** state.

1. Viewing TCAM resource usage for all stages.

   To view the TCAM resource usage for all stages (egress, ingress, and pre-ingress), use the **show pfe tcam usage all-tcam-stages detail** command.

   ```
   user@host> show pfe tcam usage all-tcam-stages detail
   ```

   ```
   Slot 0

   Tcam Resource Stage: Pre-Ingress
   --------------------------------
   ```

```
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    800       1024        224          0
Counters        800       1024        224          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
cfm-filter                500      500        0          3     OK
cfm-bd-filter             300      300        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    500        512         12          0
Counters        500       1024        524          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
fw-l2-in                  500      500        0          2     OK
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    200        512        312          0
Counters        200        512        312          0
Policers        100        512        412          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
```

```
-------------------------------------------------------------------
fw-ifl-in                 200      200      100          1     OK

Tcam Resource Stage: Egress
---------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

2. Configure additional Layer 2 services on the router.

   For example, add 20 more services on the router, thereby increasing the total number of services to 120. After adding more services, you can check the status of the configuration by verifying either the syslog message using the command **show log messages**, or by running the **show pfe tcam errors** command.

   The following is a sample syslog message output showing the TCAM resource shortage for Ethernet-switching family filters for newer configurations by running the **show log messages** CLI command.

```
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error
(dfw):acx_dfw_check_phy_slice_availability :Insufficient phy slices to accomodate
 grp:13/IN_IFF_BRIDGE mode:1/DOUBLE
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error
(dfw):acx_dfw_check_resource_availability :Could not write filter:
f-bridge-ge-0/0/0.103-i, insufficient TCAM resources
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_update_filter_in_hw
 :acx_dfw_check_resource_availability failed for filter:f-bridge-ge-0/0/0.103-i
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_create_hw_instance
:Status:1005 Could not program dfw(f-bridge-ge-0/0/0.103-i) type(IN_IFF_BRIDGE)!
 [1005]
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_bind_shim :[1005]
Could not create dfw(f-bridge-ge-0/0/0.103-i) type(IN_IFF_BRIDGE)
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_bind :[1000] bind
failed for filter f-bridge-ge-0/0/0.103-i
```

If you use the **show pfe tcam errors all-tcam-stages detail** CLI command to verify the status of the configuration, the output will be as shown below:

`user@host>` **show pfe tcam errors all-tcam-stages detail**

```
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
```

```
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    960       1024         64          0
Counters        960       1024         64          0
Policers          0       1024       1024          0

App tcam usage:
---------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
cfm-filter                600      600        0          3     OK
cfm-bd-filter             360      360        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    510        512          2         18
Counters        510       1024        514          0
Policers          0       1024       1024          0

App tcam usage:
---------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
fw-l2-in                  510      510        0          2 FAILED
  fw-semantics              0        X        X          1     OK

App error statistics:
---------------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
fw-l2-in                   18        0        0          2 FAILED
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
```

```
Tcam-Entries    240        512        272          0
Counters        240        512        272          0
Policers        120        512        392          0

App tcam usage:
---------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-ifl-in                 240      240      120          1     OK

Tcam Resource Stage: Egress
---------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

The output indicates that the **fw-l2-in** application is running out of TCAM resources and moves into a FAILED state. Although there are two TCAM slices available at the ingress stage, the **fw-l2-in** application is not able to use the available TCAM space due to its mode (DOUBLE), resulting in resource shortage failure.

3. Fixing the applications that have failed due to the shortage of TCAM resouces.

   The **fw-l2-in** application failed because of adding more number of services on the routers, which resulted in shortage of TCAM resources. Although other applications seems to work fine, it is recommended to deactivate or remove the newly added services so that the **fw-l2-in** application moves to an OK state. After removing or deactivating the newly added services, you need to run the **show pfe tcam usage** and **show pfe tcam error** commands to verify that there are no more applications in failed state.

   To view the TCAM resource usage for all stages (egress, ingress, and pre-ingress), use the **show pfe tcam usage all-tcam-stages detail** command.

   `user@host>` **show pfe tcam usage all-tcam-stages detail**

```
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
```

```
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    800       1024        224          0
Counters        800       1024        224          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
cfm-filter                500      500        0          3     OK
cfm-bd-filter             300      300        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    500        512         12         18
Counters        500       1024        524          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
fw-l2-in                  500      500        0          2     OK
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    200        512        312          0
Counters        200        512        312          0
Policers        100        512        412          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
fw-ifl-in                 200      200      100          1     OK

Tcam Resource Stage: Egress
---------------------------
```

```
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

To view TCAM resource usage errors for all stages (egress, ingress, and pre-ingress), use the **show pfe tcam errors all-tcam-stages** command.

`user@host>` **show pfe tcam errors all-tcam-stages detail**

```
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
No tcam usage

Tcam Resource Stage: Ingress
----------------------------
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Errors   Resource-Shortage
Tcam-Entries        0                  0
Counters            0                  0
Policers            0                  0

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Errors   Resource-Shortage
Tcam-Entries       18                  0
Counters            0                  0
Policers            0                  0

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Errors   Resource-Shortage
Tcam-Entries        0                  0
Counters            0                  0
Policers            0                  0

Tcam Resource Stage: Egress
---------------------------
No tcam usage
```

You can see that all the applications using the TCAM resources are in **OK** state and indicates that the hardware has been successfully configured.

> **NOTE:** As shown in the example, you will need to run the **show pfe tcam errors** and **show pfe tcam usage** commands at each step to ensure that your configurations are valid and that the applications using TCAM resource are in OK state.

Service Scaling on ACX5048 and ACX5096 Routers

In ACX5048 and ACX5096 routers, a typical service (such as ELINE, ELAN and IP VPN) that is deployed might require applications (such as policers, firewall filters, connectivity fault management IEEE 802.1ag, RFC2544) that uses the dynamic TCAM infrastructure.

> **NOTE:** Service applications that uses TCAM resources is limited by the TCAM resource availability. Therefore, the scale of the service depends upon the consumption of the TCAM resource by such applications.

A sample use case for monitoring and troubleshooting service scale in ACX5048 and ACX5096 routers can be found at the "Dynamic Ternary Content Addressable Memory Overview" on page 1599 section.

RELATED DOCUMENTATION

Understanding and Configuring the Unified Forwarding Table

IN THIS SECTION

- Using the Unified Forwarding Table to Optimize Address Storage | **1612**
- Configuring the Unified Forwarding Table to Optimize Address Storage Using Profiles | **1614**

Using the Unified Forwarding Table to Optimize Address Storage

ACX5048 and ACX5096 routers support the use of a unified forwarding table to optimize address storage. This feature gives you the flexibility to configure your router to match the needs of your particular network environment. You can control the allocation of forwarding table memory available to store the following entries:

- MAC addresses
- Layer 3 host entries
- Longest prefix match (LPM) table entries

You can use five predefined profiles (**l2-profile-one, l2-profile-two, l2-profile-three, l3-profile, lpm-profile**) to allocate the table memory space differently for each of these entries. The sizes of the Layer 2 MAC address table, Layer 3 host entry table, and Layer 3 LPM table are decided based on the selected profile. You can configure and select the profiles that best suits your network environment needs.

Table 181 on page 1612 illustrates the predefined profiles in the unified forwarding table and the respective table sizes.

Table 181: Unified Forwarding Table Profiles

Profile	Layer 2 MAC Address Table	Layer 3 Host Table	Layer 3 LPM Table
l2-profile-one	288 K	16 K	16 K
l2-profile-two	224 K	80 K	16 K
l2-profile-three (default)	160 K	144 K	16 K
l3-profile	96 K	208 K	16 K
lpm-profile	32 K	16 K	128 K

IPv4 unicast, IPv6 unicast, IPv4 multicast, and IPv6 multicast route addresses share the Layer 3 host entry table. If the host table stores the maximum number of entries for any given type, the entire table is full and is unable to accommodate any entries of any other type. The IPv4 multicast and IPv6 unicast addresses occupy double the space as that occupied by IPv4 unicast entries, and IPv6 multicast addresses occupy four times the space of the IPv4 unicast addresses. Table 182 on page 1613 shows the Layer 3 host table size for each profile.

Table 182: Layer 3 Host Table

Profile	Layer 3 Host Table			
	IPv4 Unicast	IPv4 Multicast	IPv6 Unicast	IPv6 Multicast
l2-profile-one	16 K	8 K	8 K	4 K
l2-profile-two	80 K	40 K	40 K	20 K
l2-profile-three (default)	144 K	72 K	72 K	36 K
l3-profile	208 K	104 K	104 K	52 K
lpm-profile	16 K	8 K	8 K	4 K

The Layer 3 LPM table is shared between IPv4 route prefixes and IPv6 route prefixes. Table 183 on page 1613 illustrates the size of the table for different profiles of the IPv4 and IPv4 addresses in the Layer 3 LPM table. When unicast reverse-path forwarding (unicast RPF) is enabled, the table size reduces to half.

Table 183: Layer 3 LPM Table

Profile	Layer 3 LPM Table		
	IPv4 Unicast	IPv6 Unicast (Prefix <= /64)	IPv6 Unicast (Prefix > /64)
l2-profile-one	16 K	8 K	4 K
l2-profile-two	16 K	8 K	4 K
l2-profile-three (default)	16 K	8 K	4 K
l3-profile	16 K	8 K	4 K
lpm-profile	128 K	40 K	8 K

By default, there is no space allocated for IPv6 prefix address longer than /64 in the LPM table. Therefore, prefix address longer than /64 are not allowed in the table by default. The entire table is available for IPv4 addresses and for IPv6 addresses that have prefixes shorter than /64. You can provide space in the table for addresses with prefixes longer than /64 by using CLI configuration. The number of entries reserved for these prefixes is configured in multiples of 16.

Configuring the Unified Forwarding Table to Optimize Address Storage Using Profiles

You can use five predefined profiles (**l2-profile-one, l2-profile-two, l2-profile-three, l3-profile, lpm-profile**) to allocate the table memory space. The sizes of the Layer 2 MAC address table, Layer 3 host entry table, and Layer 3 LPM table are decided based on the selected profile. You can configure and select the profiles that best suits your network environment needs.

To configure the profile that you want, enter and commit the following statement:

```
[edit]
user@host# set chassis forwarding-options profile-name profile-name
```

> **NOTE:** When you configure and commit a profile, the Packet Forwarding Engine (PFE) process restarts and all the data interfaces on the router go down and come back up.

The settings for **l2-profile-three** are configured by default. That is, if you do not configure the **forwarding–options chassis *profile-name*** statement, the **l2-profile-three** profile settings are configured.

Troubleshooting and Monitoring TCAM Resource in ACX Series Routers

The dynamic allocation of Ternary Content Addressable Memory (TCAM) space in ACX Series efficiently allocates the available TCAM resources for various filter applications. In the dynamic TCAM model, various filter applications (such as inet-firewall, bridge-firewall, cfm-filters, etc.) can optimally utilize the available TCAM resources as and when required. Dynamic TCAM resource allocation is usage driven and is dynamically allocated for filter applications on a need basis. When a filter application no longer uses the TCAM space, the resource is freed and available for use by other applications. This dynamic TCAM model caters to higher scale of TCAM resource utilization based on application's demand. You can use the show and clear commands to monitor and troubleshoot dynamic TCAM resource usage in ACX Series routers.

> **NOTE:** Applications using the TCAM resource is termed tcam-app in this document.

Table 184 on page 1615 shows the task and the commands to monitor and troubleshoot TCAM resources in ACX Series routers

Table 184: Commands to Monitor and Troubleshoot TCAM Resource in ACX Series

How to	Command
View the shared and the related applications for a particular application.	**show pfe tcam app (*list-shared-apps* | *list-related-apps*)**
View the number of applications across all tcam stages.	**show pfe tcam usage all-tcam-stages**
View the number of applications using the TCAM resource at a specified stage.	**show pfe tcam usage tcam-stage (*ingress* | *egress* | *pre-egress*)**
View the TCAM resource used by an application in detail.	**show pfe tcam usage app <*application-name*> detail**
View the TCAM resource used by an application at a specified stage.	**show pfe tcam usage tcam-stage (*ingress* | *egress* | *pre-egress*) app <*application-name*>**
Know the number of TCAM resource consumed by a tcam-app	**show pfe tcam usage app <*application-name*>**
View the TCAM resource usage errors for all stages.	**show pfe tcam errors all-tcam-stages detail**
View the TCAM resource usage errors for a stage	**show pfe tcam errors tcam-stage (*ingress* | *egress* | *pre-egress*)**
View the TCAM resource usage errors for an application.	**show pfe tcam errors app <*application-name*>**
View the TCAM resource usage errors for an application along with its other shared application.	**show pfe tcam errors app <*application-name*> shared-usage**
Clear the TCAM resource usage error statistics for all stages.	**clear pfe tcam-errors all-tcam-stages**
Clear the TCAM resource usage error statistics for a specified stage	**clear pfe tcam-errors tcam-stage (*ingress* | *egress* | *pre-egress*)**
Clear the TCAM resource usage error statistics for an application.	**clear pfe tcam-errors app <*application-name*>**

To know more about dynamic TCAM in ACX Series, see “Dynamic Ternary Content Addressable Memory Overview” on page 1599.

CHAPTER 54

Troubleshooting of System Performance with Resource Monitoring Methodology

IN THIS CHAPTER

- Resource Monitoring Usage Computation Overview | **1616**
- Diagnosing and Debugging System Performance by Configuring Memory Resource Usage Monitoring on MX Series Routers | **1619**
- Troubleshooting the Mismatch of jnxNatObjects Values for MS-DPC and MS-MIC | **1622**
- Managed Objects for Ukernel Memory for a Packet Forwarding Engine in an FPC Slot | **1624**
- Managed Objects for Packet Forwarding Engine Memory Statistics Data | **1624**
- Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot | **1625**
- jnxPfeMemoryErrorsTable | **1625**
- pfeMemoryErrors | **1626**

Resource Monitoring Usage Computation Overview

You can configure the resource monitoring capability using both the CLI and SNMP MIB queries. You can employ this utility to provision sufficient headroom (memory space limits that are set for the application or virtual router) for monitoring the health and operating efficiency of DPCs and MPCs. You can also analyze and view the usage or consumption of memory for the jtree memory type and for contiguous pages, double words, and free memory pages. The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. As the allocation of more memory for routing tables or firewall filters might disrupt the forwarding operations of a Packet Forwarding Engine, the Junos OS CLI displays a warning to restart all affected FPCs when you commit a configuration that includes the memory-enhanced route statement.

The following sections describe the computation equations and the interpretation of the different memory regions for I-chip-based and Trio-based line cards:

Resource Monitoring and Usage Computation For Trio-Based Line Cards

In Trio-based line cards, memory blocks for next-hop and firewall filters are allocated separately. Also, an expansion memory is present, which is used when the allocated memory for next-hop or firewall filter is fully consumed. Both next-hop and firewall filters can allocate memory from the expansion memory. The encapsulation memory region is specific to I-chip-based line cards and it is not applicable to Trio-based line cards. Therefore, for Trio-based line cards, the percentage of free memory space can be interpreted as follows:

% Free (NH) = (1- (Used NH memory + Used Expansion memory) / (Total NH memory+Total Expansion memory)) × 100

% Free (Firewall or Filter) = (1-(Used FW memory+Used Expansion memory) / (Total FW memory+Total Expansion memory)) × 100

Encapsulation memory is I-chip-specific and is not applicable for Trio-based line cards.

% Free (Encap memory) = Not applicable

Resource Monitoring and Usage Computation For I-Chip-Based Line Cards

I-chip-based line cards contain 32 MB of static RAM (SRAM) memory associated with the route lookup block and 16 MB of SRAM memory associated with the output WAN block.

The route-lookup memory is a single pool of 32 MB memory that is divided into two segments of 16 MB each. In a standard configuration, segment 0 is used for NH and prefixes, and segment 1 is used for firewall or filter. This allocation can be modified by using the route-memory-enhanced option at the [edit chassis] hierarchy level. In a general configuration, NH application can be allocated memory from any of the two segments. Therefore, the percentage of free memory for NH is calculated on 32 MB memory. Currently, firewall applications are allotted memory only from segment 1. As a result, the percentage of free memory to be monitored for firewall starts from the available 16 MB memory in segment 1 only.

For I-chip-based line cards, the percentage of free memory space can be interpreted as follows:

% Free (NH) = (32-(Used NH memory+Used FW memory+Used Other application)) / 32×100

% Free (Firewall or Filter)=(16-(Used NH memory+Used FW memory+Used Other application)) / 16×100

The memory size for Output WAN (Iwo) SRAM is 16 MB and stores the Layer 2 descriptors that contain the encapsulation information. This entity is a critical resource and needs to be monitored. This memory space is displayed in the output of the show command as “Encap mem”. The percentage of free memory for the encapsulation region is calculated as follows:

% Free (Encapsulation memory) = (16-(Iwo memory used (L2 descriptors +other applications))) / 16×100

The watermark level configured for next-hop memory is also effective for encapsulation memory. Therefore, if the percentage of free memory for encapsulation region falls below the configured watermark, logs are generated.

If the free memory percentage is lower than the free memory watermark of a specific memory type, the following error message is recorded in the syslog:

“Resource Monitor: FPC <slot no> PFE <pfe inst> <“JNH memory” or “FW/ Filter memory”> is below set watermark <configured watermark>”.

You can configure resource-monitoring tracing operations by using the **traceoptions file <*filename*> flag *flag* level *level* size *bytes*** statement at the **[edit system services resource-monitor]** hierarchy level. By default, messages are written to **/var/log/rsmonlog**. The error logs associated with socket communication failure (between the Routing Engine and the Packet Forwarding Engine) are useful in diagnosing the problems in the communication between the Routing Engine and the Packet Forwarding Engine.

From the Ukern perspective, MPC5E contains only one Packet Forwarding Engine instance. The show chassis fabric plane command output displays the state of fabric plane connections to the Packet Forwarding Engine. Because two Packet Forwarding Engines exist, you notice PFE-0 and PFE-1 in the output.

```
user@host# run show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
      FPC 0
          PFE 0 :Links ok
          PFE 1 :Links ok
```

Because only one Packet Forwarding Engine instance for MPC5E exists, the output of the show system resource-monitor fpc command displays only one row corresponding to Packet Forwarding Engine instance 0.

```
user@host# run show system resource-monitor fpc
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached

                    Heap                      ENCAP mem       NH mem          FW
mem
```

```
Slot #         % Free    PFE #           % Free       % Free          % Free

     0             94              0                   NA           83
   99
```

The configured watermark is retained across GRES and unified ISSU procedures.

RELATED DOCUMENTATION

Diagnosing and Debugging System Performance by Configuring Memory Resource Usage Monitoring on MX Series Routers

Junos OS supports a resource monitoring capability using both the CLI and SNMP MIB queries. You can employ this utility to provision sufficient headroom (memory space limits that are set for the application or virtual router) for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. When the memory utilization, either the ukernel memory or ASIC memory reaches a certain threshold, the system operations compromise on the health and traffic-handling stability of the line card and such a trade-off on the system performance can be detrimental for supporting live traffic and protocols.

To configure the properties of the memory resource-utilization functionality:

1. Specify that you want to configure the monitoring mechanism for utilization of different memory resource regions.

   ```
   [edit]
   user@host# edit system services resource-monitor
   ```

   This feature is enabled by default and you cannot disable it manually.

2. Specify the high threshold value, exceeding which warnings or error logs are generated, for all the regions of memory, such as heap or ukernel, next-hop and encapsulation, and firewall filter memory.

   ```
   [edit system services resource-monitor]
   user@host# set high-threshold value
   ```

3. Specify the percentage of free memory space used for next-hops to be monitored with a watermark value.

```
[edit system services resource-monitor]
user@host# set free-nh-memory-watermark percentage
```

4. Specify the percentage of free memory space used for ukernel or heap memory to be monitored with a watermark value.

```
[edit system services resource-monitor]
user@host# set free-heap-memory- watermark percentage
```

5. Specify the percentage of free memory space used for firewall and filter memory to be monitored with a watermark value.

```
[edit system services resource-monitor]
user@host# set free-filter-memory-memory- watermark percentage
```

NOTE:

The default value and the configured value of the watermark value for the percentage of free next-hop memory also applies to encapsulation memory. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20 percent.

6. Disable the generation of error log messages when the utilization of memory resources exceeds the threshold or checkpoint levels. By default, messages are written to /var/log/rsmonlog.

```
[edit system services resource-monitor]
user@host# set no-logging
```

7. Define the resource category that you want to monitor and analyze for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. The resource category includes detailed CPU utilization, session rate, and session count statistics. You use the resource category statistics to understand the extent to which new attack objects or applications affect performance.

```
[edit system services resource-monitor]
```

```
user@host# edit resource-category jtree
```

NOTE: The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. The Junos OS provides the memory-enhanced statement to reallocate the jtree memory for routes, firewall filters, and Layer 3 VPNs.

8. Configure the type of resource as contiguous pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is contiguous page in this case.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type contiguous-pages high-threshold percentage
user@host# set resource-type contiguous-pages low-threshold percentage
```

9. Configure the type of resource as free double words (dwords) for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is free dwords in this case.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type free-dwords high-threshold percentage
user@host# set resource-type free-dwords low-threshold percentage
```

10. Configure the type of resource as free memory pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is free memory pages in this case.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type free-pages high-threshold percentage
user@host# set resource-type free-pages low-threshold percentage
```

11. View the utilization of memory resources on the Packet Forwarding Engines of an FPC by using the **show system resource-monitor fpc** command. The filter memory denotes the filter counter memory

used for firewall filter counters. The asterisk (*) displayed next to each of the memory regions denotes the ones for which the configured threshold is being currently exceeded.

```
user@host# run show system resource-monitor fpc
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached

                    Heap                      ENCAP mem       NH mem          FW
 mem
   Slot #         % Free    PFE #           % Free       % Free          % Free

        0             94             0                   NA          83
         99
```

RELATED DOCUMENTATION

Troubleshooting the Mismatch of jnxNatObjects Values for MS-DPC and MS-MIC

Problem

Description: When both MS-DPC and MS-MIC are deployed in a network and the Network Address Translation (NAT) type is configured as **napt-44**, the output of the **snmp mib walk** command for jnxNatObjects displays different values for MS-DPC and MS-MIC.

Resolution

Configure SNMP to Match jnxNatObjects Values for MS-DPC and MS-MIC

To configure SNMP to match jnxNatObjects values for MS-DPC and MS-MIC:

1. Run the **set services service-set** ***service-set-name*** **nat-options** snmp-value-match-msmic configuration mode command. The following configuration example shows how to configure

SNMP to match the values for MS-MIC-specific objects in the jnxNatObjects MIB table with the values for MS-DPC objects.

```
[edit]
user@host# set services service-set Mobile nat-options snmp-value-match-msmic
```

2. Issue the **commit** command to confirm the changes.

```
[edit]
user@host# commit
commit complete
```

3. (Optional) Run the **show snmp mib walk jnxNatObjects** command to verify that the values for MS-MIC-specific objects in the jnxNatObjects MIB table match the values for MS-DPC objects. For example, the following output shows that the values for MS-MIC-specific objects and MS-DPC objects match.

```
[edit]
user@host# run show snmp mib walk jnxNatObjects
jnxNatSrcXlatedAddrType.6.77.111.98.105.108.101 = 1
jnxNatSrcPoolType.6.77.111.98.105.108.101 = 13
jnxNatSrcNumPortAvail.6.77.111.98.105.108.101 = 64512
jnxNatSrcNumPortInuse.6.77.111.98.105.108.101 = 0
jnxNatSrcNumAddressAvail.6.77.111.98.105.108.101 = 1
jnxNatSrcNumAddressInUse.6.77.111.98.105.108.101 = 0
jnxNatSrcNumSessions.6.77.111.98.105.108.101 = 0
jnxNatRuleType.9.77.111.98.105.108.101.58.116.49 = 13
jnxNatRuleTransHits.9.77.111.98.105.108.101.58.116.49 = 0
jnxNatPoolType.6.77.111.98.105.108.101 = 13
jnxNatPoolTransHits.6.77.111.98.105.108.101 = 0
```

NOTE: You can use the **delete services service-set *service-set-name* nat-options snmp-value-match-msmic** configuration mode command to disable this feature.

RELATED DOCUMENTATION

Configuring Service Rules

snmp-value-match-msmic | 2241

Managed Objects for Ukernel Memory for a Packet Forwarding Engine in an FPC Slot

The **jnxPfeMemoryUkernTable**, whose object identifier is **{jnxPfeMemory 1}**, contains the **JnxPfeMemoryUkernEntry** that retrieves the global ukernel or heap memory statistics for the specified Packet Forwarding Engine slot. Each **JnxPfeMemoryUkernEntry**, whose object identifier is **{jnxPfeMemoryUkernTable 1}**, contains the objects listed in the following table. The **jnxPfeMemoryUkernEntry** denotes the memory utilization, such as the total available memory and the percentage of memory used.

Table 185: jnxPfeMemoryUKernTable

Object	Object ID	Description
jnxPfeMemoryUkernFreePercent	**jnxPfeMemoryUkernEntry 3**	Denotes the percentage of free Packet Forwarding Engine memory within the ukern heap.

Managed Objects for Packet Forwarding Engine Memory Statistics Data

The **jnxPfeMemory** table, whose object identifier is **{jnxPfeMib 2}** contains the objects listed in Table 186 on page 1624

Table 186: jnxPfeMemory Table

Object	Object ID	Description
jnxPfeMemoryUkernTable	**jnxPfeMemory 1**	Provides global ukern memory statistics for the specified Packet Forwarding Engine slot.
jnxPfeMemoryForwardingTable	**jnxPfeMemory 2**	Provides global next-hop (for Trio-based line cards) or Jtree (for I-chip-based line cards) memory utilization and firewall filter memory utilization statistics for the specified Packet Forwarding Engine slot.

Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot

The **jnxPfeMemoryForwardingTable**, whose object identifier is **{jnxPfeMemory 2}**, contains **JnxPfeMemoryForwardingEntry** that retrieves the next-hop memory for Trio- based line cards, jtree memory for I-chip-based line cards, and firewall or filter memory statistics for the specified Packet Forwarding Engine slot for both I- chip and Trio-based line cards. Each **jnxPfeMemoryForwardingEntry**, whose object identifier is **{jnxPfeMemoryForwardingTable 1}**, contains the objects listed in the following table.

The **jnxPfeMemoryForwardingEntry** represents the ASIC instance, ASIC memory used, and ASIC free memory. The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. As the allocation of more memory for routing tables or firewall filters might disrupt the forwarding operations of a Packet Forwarding Engine, the Junos OS CLI displays a warning to restart all affected FPCs when you commit a configuration that includes the memory-enhanced route statement. The configuration does not become effective until you restart the FPC or DPC (on MX Series routers).

Table 187: jnxPfeMemoryForwardingTable

Object	Object ID	Description
jnxPfeMemoryForwardingChipSlot	**jnxPfeMemoryForwardingEntry 1**	Indicates the ASIC instance number in the Packet Forwarding Engine complex.
jnxPfeMemoryType	**jnxPfeMemoryForwardingEntry 2**	Indicates the Packet Forwarding Engine memory type, where nh = 1, fw = 2, encap = 3.
jnxPfeMemoryForwardingPercentFree	**jnxPfeMemoryForwardingEntry 3**	Indicates the percentage of memory free for each memory type.

jnxPfeMemoryErrorsTable

The Juniper Networks enterprise-specific Packet Forwarding Engine MIB, whose object ID is **{jnxPfeMibRoot 1}**, supports a new MIB table, **jnxPfeMemoryErrorsTable**, to display Packet Forwarding Engine memory error counters. The **jnxPfeMemoryErrorsTable**, whose object identifier is **jnxPfeNotification 3**, contains the **JnxPfeMemoryErrorsEntry**. Each **JnxPfeMemoryErrorsEntry**, whose object identifier is **{ jnxPfeMemoryErrorsTable 1 }**, contains the objects listed in the following table.

Table 188: jnxPfeMemoryErrorsTable

Object	Object ID	Description
jnxPfeFpcSlot	**jnxPfeMemoryErrorsEntry 1**	Signifies the FPC slot number for this set of PFE notification
jnxPfeSlot	**jnxPfeMemoryErrorsEntry 2**	Signifies the PFE slot number for this set of errors
jnxPfeParityErrors	**jnxPfeMemoryErrorsEntry 3**	Signifies the parity error count
jnxPfeEccErrors	**jnxPfeMemoryErrorsEntry 4**	Signifies the error-checking code (ECC) error count

pfeMemoryErrors

The **pfeMemoryErrorsNotificationPrefix**, whose object identifier is **{jnxPfeNotification 0}**, contains the **pfeMemoryErrors** attribute. The pfeMemoryErrors object, whose identifier is **{pfeMemoryErrorsNotificationPrefix 1}** contains the **jnxPfeParityErrors** and **jnxPfeEccErrors** objects.

Table 189: pfeMemoryErrors

Object	Object ID	Description
pfeMemoryErrors	**pfeMemoryErrorsNotificationPrefix 1**	A pfeMemoryErrors notification is sent when the value of jnxPfeParityErrors or jnxPfeEccErrors increases.

CHAPTER 55

Configuring Data Path Debugging and Trace Options

IN THIS CHAPTER

- Understanding Data Path Debugging for SRX Series Devices | 1627
- Packet Capture from Operational Mode | 1629
- Understanding Security Debugging Using Trace Options | 1630
- Understanding Flow Debugging Using Trace Options | 1630
- Debugging the Data Path (CLI Procedure) | 1631
- Setting Flow Debugging Trace Options (CLI Procedure) | 1632
- Setting Security Trace Options (CLI Procedure) | 1633
- Displaying Log and Trace Files | 1634
- Displaying Output for Security Trace Options | 1635
- Displaying Multicast Trace Operations | 1636
- J-Web Traceroute Results and Output Summary | 1637
- Displaying a List of Devices | 1638
- Example: Configuring End-to-End Debugging on SRX Series Device | 1640

Understanding Data Path Debugging for SRX Series Devices

Data path debugging, or end-to-end debugging, support provides tracing and debugging at multiple processing units along the packet-processing path. The packet filter can be executed with minimal impact to the production system.

If your goal is to collect packet captures, we strongly recommend leveraging the Operational Mode Packet Capture introduced in Junos OS Release 19.3R1. See "Packet Capture from Operational Mode" on page 1629.

On an SRX Series device, a packet goes through series of events involving different components from ingress to egress processing.

With the data path debugging feature, you can trace and debug (capture packets) at different data points along the processing path. The events available in the packet-processing path are: NP ingress, load-balancing thread (LBT), jexec, packet-ordering thread (POT), and NP egress. You can also enable flow module trace if the security flow trace flag for a certain module is set.

At each event, you can specify any of the four actions (count, packet dump, packet summary, and trace). Data path debugging provides filters to define what packets to capture, and only the matched packets are traced. The packet filter can filter out packets based on logical interface, protocol, source IP address prefix, source port, destination IP address prefix, and destination port.

Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX4600, SRX5400, SRX5600, and SRX5800.

To enable end-to-end debugging, you must perform the following steps:

1. Define the capture file and specify the maximum capture size.
2. Define the packet filter to trace only a certain type of traffic based on the requirement.
3. Define the action profile specifying the location on the processing path from where to capture the packets (for example, LBT or NP ingress).
4. Enable the data path debugging.
5. Capture traffic.
6. Disable data path debugging.
7. View or analyze the report.

The packet-filtering behavior for the port and interface options is as follows:

- The packet filter traces both IPv4 and IPv6 traffic if only **port** is specified.
- The packet filter traces IPv4, IPV6, and non-IP traffic if only **interface** is specified.

RELATED DOCUMENTATION

Understanding Security Debugging Using Trace Options | **1630**

Understanding Flow Debugging Using Trace Options | **1630**

Debugging the Data Path (CLI Procedure) | **1631**

Example: Configuring End-to-End Debugging on SRX Series Device | **1640**

Packet Capture from Operational Mode | **1629**

Packet Capture from Operational Mode

Data path debugging or end-to-end debugging provides tracing and debugging at multiple processing units along the packet-processing path. Packet capture is one of the data path debug function. You can execute the packet capture from the operational mode with minimal impact to the production system without committing the configurations.

You can capture the packets using filters to define what packets to capture. The packet filter can filter out packets based on logical interface, protocol, source IP address prefix, source port, destination IP address prefix, and destination port. You can modify the file name, file type, file size, and capture size of the packet capture output. You can also extend the filters into two filters, and swap the values of filters.

To capture packets from the operational mode, you must perform the following steps:

1. From the operational mode, define the packet filter to trace the type of traffic based on your requirement using the **request packet-capture start** CLI command. See **request packet-capture start** for the available packet capture filter options.

2. Capture the required packets.

3. You can use either the **request packet-capture stop** CLI command to stop the packet capture or after collecting the requested number of packets, the packet capturing stops automatically.

4. View or analyze the captured packet data report.

Limitations of capturing packets from the operational mode are:

1. The configuration mode packet capture and the operational mode packet capture cannot coexist.

2. The operational mode packet capture is a one-time operation and the system does not store the history of this command.

3. You should use the operational mode packet capture in low rate of traffic flow.

RELATED DOCUMENTATION

request packet-capture start | **2972**

request packet-capture stop | **2978**

Understanding Security Debugging Using Trace Options

The Junos OS trace function allows applications to write security debugging information to a file. The information that appears in this file is based on criteria you set. You can use this information to analyze security application issues.

The trace function operates in a distributed manner, with each thread writing to its own trace buffer. These trace buffers are then collected at one point, sorted, and written to trace files. Trace messages are delivered using the InterProcess Communications (IPC) protocol. A trace message has a lower priority than that of control protocol packets such as BGP, OSPF, and IKE, and therefore delivery is not considered to be as reliable.

RELATED DOCUMENTATION

- Understanding Data Path Debugging for SRX Series Devices | 1627
- Understanding Flow Debugging Using Trace Options | 1630
- Setting Security Trace Options (CLI Procedure) | 1633
- Debugging the Data Path (CLI Procedure) | 1631
- Displaying Output for Security Trace Options | 1635

Understanding Flow Debugging Using Trace Options

For flow trace options, you can define a packet filter using combinations of **destination-port**, **destination-prefix**, **interface**, **protocol**, **source-port**, and **source-prefix**. If the security flow trace flag for a certain module is set, the packet matching the specific packet filter triggers flow tracing and writes debugging information to the trace file.

RELATED DOCUMENTATION

- Understanding Data Path Debugging for SRX Series Devices | 1627
- Understanding Security Debugging Using Trace Options | 1630
- Setting Flow Debugging Trace Options (CLI Procedure) | 1632
- Debugging the Data Path (CLI Procedure) | 1631

Debugging the Data Path (CLI Procedure)

Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

To configure the device for data path debugging:

1. Specify the following request command to set the data path debugging for the multiple processing units along the packet-processing path:

```
[edit]
user@host# set security datapath-debug
```

2. Specify the trace options for data path-debug using the following command:

```
[edit]
user@host# set security datapath-debug traceoptions
```

3. Using the request security packet-filter command, you can set the packet filter to specify the related packets to perform data path-debug action. A maximum of four filters are supported at the same time. For example, the following command sets the first packet-filter:

```
[edit]
user@host# set security datapath-debug packet-filter name
```

4. Using the request security action-profile command, you can set the action for the packet match for a specified filter. Only the default action profile is supported, which is the trace option for network processor ezchip ingress, ezchip egress, spu.lbt, and spu.pot:

```
[edit]
user@host# set security datapath-debug packet-filter name action-profile
```

RELATED DOCUMENTATION

Understanding Data Path Debugging for SRX Series Devices | 1627

Understanding Security Debugging Using Trace Options | 1630

Understanding Flow Debugging Using Trace Options | 1630

Setting Flow Debugging Trace Options (CLI Procedure) | 1632

Setting Flow Debugging Trace Options (CLI Procedure)

The following examples display the options you can set by using **security flow traceoptions**.

- To match the imap destination port for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-port imap
```

- To set the 1.2.3.4 destination IPv4 prefix address for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-prefix 1.2.3.4
```

- To set the fxp0 logical interface for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 interface fxp0
```

- To match the TCP IP protocol for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 protocol tcp
```

- To match the HTTP source port for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-port http
```

- To set the 5.6.7.8 IPv4 prefix address for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-prefix 5.6.7.8
```

RELATED DOCUMENTATION

Understanding Flow Debugging Using Trace Options | 1630

Setting Security Trace Options (CLI Procedure)

Use the following configuration statements to configure security trace options in the CLI configuration editor.

- To disable remote tracing, enter the following statement:

```
[edit]
user@host# set security traceoptions no-remote-trace
```

- To write trace messages to a local file, enter the following statement. The system saves the trace file in the **/var/log/** directory.

```
[edit]
user@host# set security traceoptions use-local-files
```

- To specify a name for the trace file, enter the following statement. Valid values range from 1 and 1024 characters. The name cannot include spaces, /, or % characters. The default filename is security.

```
[edit]
user@host# set security traceoptions file filename
```

- To specify the maximum number of trace files that can accumulate, enter the following statement. Valid values range from 2 to 1000. The default value is 3.

```
[edit]
user@host# set security traceoptions file files 3
```

- To specify the match criteria that you want the system to use when logging information to the file, enter the following statement. Enter a regular expression. Wildcard (*) characters are accepted.

```
[edit]
user@host# set security traceoptions file match *thread
```

- To allow any user to read the trace file, enter the **world-readable** statement. Otherwise, enter the **no-world-readable** statement.

```
[edit]
user@host# set security traceoptions file world-readable
user@host# set security traceoptions file no-world-readable
```

- To specify the maximum size to which the trace file can grow, enter the following statement. Once the file reaches the specified size, it is compressed and renamed *filename*0.gz, the next file is named *filename*1.gz, and so on. Valid values range from 10240 to 1,073,741,824.

```
[edit]
user@host# set security traceoptions file size 10240
```

- To turn on trace options and to perform more than one tracing operation, set the following flags.

```
[edit]
user@host# set security traceoptions flag all
user@host# set security traceoptions flag compilation
user@host#  set security traceoptions flag configuration
user@host# set security traceoptions flag routing-socket
```

- To specify the groups that these trace option settings do or do not apply to, enter the following statements:

```
[edit]
user@host# set security traceoptions apply-groups value
user@host# set security traceoptions apply-groups-except value
```

RELATED DOCUMENTATION

Understanding Security Debugging Using Trace Options | 1630

Displaying Output for Security Trace Options | 1635

Displaying Log and Trace Files

Enter the **monitor start** command to display real-time additions to system logs and trace files:

```
user@host> monitor start filename
```

When the device adds a record to the file specified by ***filename***, the record displays on the screen. For example, if you have configured a system log file named **system-log** (by including the **syslog** statement at the [**edit system**] hierarchy level), you can enter the **monitor start system-log** command to display the records added to the system log.

To display a list of files that are being monitored, enter the **monitor list** command. To stop the display of records for a specified file, enter the **monitor stop *filename*** command.

RELATED DOCUMENTATION

Displaying a List of Devices | **1638**

Displaying Real-Time Monitoring Information | **1057**

Displaying Output for Security Trace Options

Purpose

Display output for security trace options.

Action

Use the **show security traceoptions** command to display the output of your trace files. For example:

```
[edit]
user@host # show security traceoptions file usp_trace
user@host # show security traceoptions flag all
user@host # show security traceoptions rate-limit 888
```

The output for this example is as follows:

```
Apr 11 16:06:42 21:13:15.750395:CID-906489336:FPC-01:PIC-01:THREAD_ID-01:PFE:now update
  0x3607edf8df8in 0x3607e8d0
Apr 11 16:06:42 21:13:15.874058:CID-1529687608:FPC-01:PIC-01:THREAD_ID-01:CTRL:Enter
  Function[util_ssam_handler]
Apr 11 16:06:42 21:13:15.874485:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1: Rate limit changed
  to 888
Apr 11 16:06:42 21:13:15.874538:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1: Destination ID set
  to 1
Apr 11 16:06:42 21:13:15.874651:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2: Rate limit changed
  to 888
Apr 11 16:06:42 21:13:15.874832:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2: Destination ID set
  to 1
Apr 11 16:06:42 21:13:15.874942:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3: Rate limit changed
  to 888
Apr 11 16:06:42 21:13:15.874997:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3: Destination ID set
  to 1
```

RELATED DOCUMENTATION

Understanding Security Debugging Using Trace Options | 1630

Setting Security Trace Options (CLI Procedure) | 1633

Displaying Multicast Trace Operations

To monitor and display multicast trace operations, enter the **mtrace monitor** command:

```
user@host> mtrace monitor
```

```
Mtrace query at Apr 21 16:00:54 by 192.1.30.2, resp to 224.0.1.32, qid 2a83aa
packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to 192.1.4.1 via group 224.1.1.1
 (mxhop=60)  Mtrace query at Apr 21 16:00:57 by 192.1.30.2, resp to 224.0.1.32,
qid 25dc17 packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to 192.1.4.1 via
group 224.1.1.1 (mxhop=60)  Mtrace query at Apr 21 16:01:00 by 192.1.30.2, resp
to same, qid 20e046 packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to 192.1.4.1
 via group 224.1.1.1 (mxhop=60)  Mtrace query at Apr 21 16:01:10 by 192.1.30.2,
resp to same, qid 1d25ad packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to
192.1.4.1 via group 224.1.1.1 (mxhop=60)
```

This example displays only **mtrace** queries. However, when the device captures an **mtrace** response, the display is similar, but the complete **mtrace** response also appears (exactly as it is appears in the **mtrace from-source** command output).

Table 190 on page 1636 summarizes the output fields of the display.

Table 190: CLI mtrace monitor Command Output Summary

Field	Description
Mtrace *operation-type* at *time-of-day*	• ***operation-type***—Type of multicast trace operation: **query** or **response**. • ***time-of-day***—Date and time the multicast trace query or response was captured.
by	IP address of the host issuing the query.
resp to *address*	***address***—Response destination address.
qid *qid*	***qid***—Query ID number.

Table 190: CLI mtrace monitor Command Output Summary *(continued)*

Field	Description
packet from *source* to *destination*	• ***source***—IP address of the source of the query or response. • ***destination***—IP address of the destination of the query or response.
from *source* to *destination*	• ***source***—IP address of the multicast source. • ***destination***—IP address of the multicast destination.
via group *address*	***address***—Group address being traced.
mxhop=*number*	***number***—Maximum hop setting.

RELATED DOCUMENTATION

Using the J-Web Traceroute Tool

J-Web Traceroute Results and Output Summary | **1637**

J-Web Traceroute Results and Output Summary

Table 191 on page 1637 summarizes the output in the traceroute display.

Table 191: J-Web Traceroute Results and Output Summary

Field	Description
hop-number	Number of the hop (device) along the path.
host	Hostname, if available, or IP address of the device. If the Don't Resolve Addresses check box is selected, the hostname does not appear.
ip-address	IP address of the device.
as-number	AS number of the device.
time1	Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.
time2	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.

Table 191: J-Web Traceroute Results and Output Summary *(continued)*

Field	Description
time3	Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.

If the device does not display the complete path to the destination host, one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host, or a router along the path, might be configured to ignore ICMP traceroute messages.
- The host, or a device along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses.
- The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message.

RELATED DOCUMENTATION

Diagnostic Tools Overview | 16

Using the J-Web Traceroute Tool

Displaying a List of Devices

To display a list of devices between the device and a specified destination host, enter the **traceroute** command with the following syntax:

```
user@host> traceroute host <interface interface-name> <as-number-lookup> <bypass-routing> <gateway address>
  <inet | inet6> <no-resolve> <routing-instance routing-instance-name> <source source-address> <tos number>
  <ttl number> <wait seconds>
```

Table 192 on page 1638 describes the **traceroute** command options.

Table 192: CLI traceroute Command Options

Option	Description
host	Sends traceroute packets to the hostname or IP address you specify.

Table 192: CLI traceroute Command Options *(continued)*

Option	Description
interface *interface-name*	(Optional) Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.
as-number-lookup	(Optional) Displays the autonomous system (AS) number of each intermediate hop between the device and the destination host.
bypass-routing	(Optional) Bypasses the routing tables and sends the traceroute packets only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. Use this option to display a route to a local system through an interface that has no route through it.
gateway *address*	(Optional) Uses the gateway you specify to route through.
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
routing-instance *routing-instance-name*	(Optional) Uses the routing instance you specify for the traceroute.
source *address*	(Optional) Uses the source address that you specify, in the traceroute packet.
tos *number*	(Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from **0** through **255**.
ttl *number*	(Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from **0** through **128**.
wait *seconds*	(Optional) Sets the maximum time to wait for a response.

To quit the **traceroute** command, press Ctrl-C.

The following is sample output from a **traceroute** command:

```
user@host> traceroute host2
```

```
traceroute to 173.24.232.66 (172.24.230.41), 30 hops max, 40 byte packets  1
173.18.42.253 (173.18.42.253)  0.482 ms  0.346 ms  0.318 ms  2  host4.site1.net
(173.18.253.5)  0.401 ms  0.435 ms  0.359 ms  3  host5.site1.net (173.18.253.5)
0.401 ms  0.360 ms  0.357 ms  4  173.24.232.65 (173.24.232.65)  0.420 ms  0.456
ms  0.378 ms  5  173.24.232.66 (173.24.232.66)  0.830 ms  0.779 ms  0.834 ms
```

The fields in the display are the same as those displayed by the J-Web traceroute diagnostic tool.

RELATED DOCUMENTATION

Displaying Log and Trace Files | 1634

Example: Configuring End-to-End Debugging on SRX Series Device

IN THIS SECTION

- Requirements | 1640
- Overview | 1641
- Configuration | 1641
- Enabling Data Path Debugging | 1643
- Verification | 1644

This example shows how to configure and enable end-to-end debugging on an SRX Series device with an SRX5K-MPC.

Requirements

This example uses the following hardware and software components:

- SRX5600 device with an SRX5K-MPC installed with 100-Gigabit Ethernet CFP transceiver
- Junos OS Release 12.1X47-D15 or later for SRX Series devices

Before you begin:

- See *Understanding Data Path Debugging for SRX Series Devices*.

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

Overview

Data path debugging enhances troubleshooting capabilities by providing tracing and debugging at multiple processing units along the packet-processing path. With the data path debugging feature, you can trace and debug (capture packets) at different data points along the processing path. At each event, you can specify an action (count, packet dump, packet summary, and trace) and you can set filters to define what packets to capture.

In this example, you define a traffic filter, and then you apply an action profile. The action profile specifies a variety of actions on the processing unit. The ingress and egress are specified as locations on the processing path to capture the data for incoming and outgoing traffic.

Next, you enable data path debugging in operational mode, and finally you view the data capture report.

> **NOTE:** Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

Configuration

CLI Quick Configuration

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

```
set security datapath-debug traceoptions file e2e.trace size 10m
set security datapath-debug capture-file e2e.pcap format pcap
set security datapath-debug maximum-capture-size 1500
set security datapath-debug capture-file files 10
set security datapath-debug action-profile profile-1 preserve-trace-order
set security datapath-debug action-profile profile-1 record-pic-history
set security datapath-debug action-profile profile-1 event np-ingress trace
set security datapath-debug action-profile profile-1 event np-ingress count
set security datapath-debug action-profile profile-1 event np-ingress packet-summary
set security datapath-debug action-profile profile-1 event np-egress trace
set security datapath-debug action-profile profile-1 event np-egress count
```

```
set security datapath-debug action-profile profile-1 event np-egress packet-summary
```

Step-by-Step Procedure

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

To configure data path debugging:

1. Edit the security datapath debugging option for the multiple processing units along the packet-processing path:

```
[edit]
user@host# edit security datapath-debug
```

2. Enable the capture file, file format, file size, and the number of files.

```
[edit security datapath-debug]
user@host# set traceoptions file e2e.trace size 10m
user@host# set capture-file e2e.pcap format pcap;
user@host# set maximum-capture-size 1500
user@host# set capture-file files 10
```

3. Configure action profile, event type, and actions for the action profile.

```
[edit security datapath-debug]
user@host# set action-profile profile-1 preserve-trace-order
user@host# set action-profile profile-1 record-pic-history
user@host# set action-profile profile-1 event np-ingress trace
user@host# set action-profile profile-1 event np-ingress count
user@host# set action-profile profile-1 event np-ingress packet-summary
user@host# set action-profile profile-1 event np-egress trace
user@host# set action-profile profile-1 event np-egress count
user@host# set action-profile profile-1 event np-egress packet-summary
```

Results

From configuration mode, confirm your configuration by entering the **show security datapath-debug** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
traceoptions {
```

```
    file e2e.trace size 10m;
}
capture-file e2e.pcap format pcap;
maximum-capture-size 1500;
capture-file files 10;
action-profile {
    profile-1 {
        preserve-trace-order;
        record-pic-history;
        event np-ingress {
            trace;
            packet-summary;
            packet-dump;
        }
        event np-egress {
            trace;
            packet-summary;
            packet-dump;
        }
    }
}
```

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

Enabling Data Path Debugging

Step-by-Step Procedure

After configuring data path debugging, you must start the process on the device from operational mode.

1. Enable data path debugging.

   ```
   user@host> request security datapath-debug capture start
   ```

   ```
   datapath-debug capture started on file datapcap
   ```

2. Before you verify the configuration and view the reports, you must disable data path debugging.

   ```
   user@host> request security datapath-debug capture stop
   ```

```
datapath-debug capture succesfully stopped, use show security datapath-debug
capture to view
```

NOTE: You must stop the debug process after you have finished capturing the data. If you attempt to open the captured files without stopping the debug process, the files obtained cannot be opened through any third-party software (for example, tcpdump and wireshark).

Verification

Confirm that the configuration is working properly.

Verifying Data Path Debug Packet Capture Details

Purpose

Verify the data captured by enabling the data path debugging configuration.

Action

From operational mode, enter the **show security datapath-debug capture** command.

```
Packet 8, len 152: (C2/F2/P0/SEQ:57935:np-ingress)
00 10 db ff 10 02 00 30 48 83 8d 4f 08 00 45 00
00 54 00 00 40 00 40 01 9f c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37
Packet 9, len 152: (C2/F2/P0/SEQ:57935:np-egress)
00 30 48 8d 1a bf 00 10 db ff 10 03 08 00 45 00
00 54 00 00 40 00 3f 01 a0 c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37....
```

For brevity, the **show** command output is truncated to display only a few samples. Additional samples have been replaced with ellipses (...).

To view the results, from CLI operational mode, access the local UNIX shell and navigate to the directory **/var/log/<*file-name*>**. The result can be read by using the **tcpdump** utility.

```
user@host>start shell
%tcpdump -nr/var/log/e2e.pcap
```

```
21:50:04.288767 C0/F3 event:1(np-ingress) SEQ:1 IP 192.168.14.2 > 192.168.13.2:
ICMP echo request, id 57627, seq 0, length 64
21:50:04.292590 C0/F3 event:2(np-egress) SEQ:1 IP 192.168.14.2 > 192.168.13.2:
ICMP echo request, id 57627, seq 0, length 64
1:50:04.295164 C0/F3 event:1(np-ingress) SEQ:2 IP 192.168.13.2 > 192.168.14.2:
ICMP echo reply, id 57627, seq 0, length 64
21:50:04.295284 C0/F3 event:2(np-egress) SEQ:2 IP 192.168.13.2 > 192.168.14.2:
ICMP echo reply, id 57627, seq 0, length 64
```

NOTE: If you are finished with troubleshooting the data path debugging, remove all **traceoptions** (not limited to flow traceoptions) and the complete data path debug configuration, including the data path debug configuration for packet capturing (packet-dump), which needs to be started/stopped manually. If any part of the debugging configuration remains active, it will continue to use the resources of the device (CPU/memory).

RELATED DOCUMENTATION

Understanding Data Path Debugging for SRX Series Devices | **1627**

Packet Capture from Operational Mode | **1629**

CHAPTER 56

Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits

IN THIS CHAPTER

- MPLS Connection Checking Overview | **1646**
- Understanding Ping MPLS | **1649**
- Using the ping Command | **1650**
- Pinging Layer 2 Circuits | **1653**
- Pinging Layer 2 VPNs | **1654**
- Pinging Layer 3 VPNs | **1656**
- Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | **1657**

MPLS Connection Checking Overview

Use either the J-Web ping MPLS diagnostic tool or the CLI commands **ping mpls**, **ping mpls l2circuit**, **ping mpls l2vpn**, and **ping mpls l3vpn** to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits.

Based on how the LSP or VPN outbound (egress) node at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP or VPN.

Each probe is an echo request sent to the LSP or VPN exit point as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the device receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

Table 193 on page 1647 summarizes the options for using either the J-Web ping MPLS diagnostic tool or the CLI **ping mpls** command to display information about MPLS connections in VPNs and LSPs.

Table 193: Options for Checking MPLS Connections

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping RSVP-signaled LSP	**ping mpls rsvp**	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The device pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the device sends the ping requests on the path that is currently active.
Ping LDP-signaled LSP	**ping mpls ldp**	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The device pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the device sends the ping requests through the first gateway. Ping requests sent to LDP-signaled LSPs use only the master routing instance.
Ping LSP to Layer 3 VPN prefix	**ping mpls l3vpn**	Checks the operability of the connections related to a Layer 3 VPN. The device tests whether a prefix is present in a provider edge (PE) device's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix.	The device does not test the connection between a PE device and a customer edge (CE) router.
Locate LSP using interface name	**ping mpls l2vpn interface**	Checks the operability of the connections related to a Layer 2 VPN. The device directs outgoing request probes out the specified interface.	–
Instance to which this connection belongs	**ping mpls l2vpn instance**	Checks the operability of the connections related to a Layer 2 VPN. The device pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, to test the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound and outbound PE routers.	–

Table 193: Options for Checking MPLS Connections *(continued)*

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Locate LSP from interface name	**ping mpls l2circuit interface**	Checks the operability of the Layer 2 circuit connections. The device directs outgoing request probes out the specified interface.	–
Locate LSP from virtual circuit information	**ping mpls l2circuit virtual-circuit**	Checks the operability of the Layer 2 circuit connections. The device pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE router, testing the integrity of the Layer 2 circuit between the inbound and outbound PE routers.	–
Ping end point of LSP	**ping mpls lsp-end-point**	Checks the operability of an LSP endpoint. The device pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address.	–

RELATED DOCUMENTATION

Diagnostic Tools Overview | **16**

Understanding Ping MPLS | **1649**

Using the J-Web Ping Host Tool

Using the ping Command | **1650**

Understanding Ping MPLS

IN THIS SECTION

- MPLS Enabled | 1649
- Loopback Address | 1649
- Source Address for Probes | 1649

Before using the ping MPLS feature, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and that the loopback interface on the outbound node is configured as **127.0.0.1**. The source address for MPLS probes must be a valid address on the J Series device.

This section includes the following topics:

MPLS Enabled

To process ping MPLS requests, the remote endpoint of the VPN or LSP must be configured appropriately. You must enable MPLS on the receiving interface of the outbound node for the VPN or LSP. If MPLS is not enabled, the remote endpoint drops the incoming request packets and returns an “ICMP host unreachable” message to the J Series device.

Loopback Address

The loopback address (**lo0**) on the outbound node must be configured as **127.0.0.1**. If this interface address is not configured correctly, the outbound node does not have this forwarding entry. It drops the incoming request packets and returns a “host unreachable” message to the J Series device.

Source Address for Probes

The source IP address you specify for a set of probes must be an address configured on one of the J Series device interfaces. If it is not a valid J Series device address, the ping request fails with the error message “Can't assign requested address.”

RELATED DOCUMENTATION

- Diagnostic Tools Overview | 16
- MPLS Connection Checking Overview | 1646

Using the J-Web Ping Host Tool

Using the J-Web Ping MPLS Tool

Using the ping Command | **1650**

Junos OS Interfaces Configuration Guide for Security Devices

Junos OS Feature Support Reference for SRX Series and J Series Devices

Using the ping Command

You can perform certain tasks only through the CLI. Use the CLI **ping** command to verify that a host can be reached over the network. This command is useful for diagnosing host and network connectivity problems. The device sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Enter the **ping** command with the following syntax:

```
user@host> ping host <interface source-interface> <bypass-routing> <count number> <do-not-fragment> <inet
  | inet6> <interval seconds> <loose-source [hosts]> <no-resolve> <pattern string> <rapid> <record-route>
  <routing-instance routing-instance-name> <size bytes> <source source-address> <strict> <strict-source [hosts]>
  <tos number> <ttl number> <wait seconds> <detail> <verbose>
```

Table 194 on page 1650 describes the **ping** command options.

To quit the **ping** command, press Ctrl-C.

Table 194: CLI ping Command Options

Option	Description
host	Pings the hostname or IP address you specify.
interface *source-interface*	(Optional) Sends the ping requests on the interface you specify. If you do not include this option, ping requests are sent on all interfaces.
bypass-routing	(Optional) Bypasses the routing tables and sends the ping requests only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. Use this option to ping a local system through an interface that has no route through it.
count*number*	(Optional) Limits the number of ping requests to send. Specify a count from **1** through **2,000,000,000**. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.

Table 194: CLI ping Command Options *(continued)*

Option	Description
do-not-fragment	(Optional) Sets the Don't Fragment (DF) bit in the IP header of the ping request packet.
inet	(Optional) Forces the ping requests to an IPv4 destination.
inet6	(Optional) Forces the ping requests to an IPv6 destination.
interval ***seconds***	(Optional) Sets the interval between ping requests, in seconds. Specify an interval from **0.1** through **10,000**. The default value is **1** second.
loose-source [*hosts*]	(Optional) For IPv4, sets the loose source routing option in the IP header of the ping request packet.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
pattern ***string***	(Optional) Includes the hexadecimal string you specify, in the ping request packet.
rapid	(Optional) Sends ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the **count** option.
record-route	(Optional) For IPv4, sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed on the screen.
routing-instance ***routing-instance-name***	(Optional) Uses the routing instance you specify for the ping request.
size ***bytes***	(Optional) Sets the size of the ping request packet. Specify a size from **0** through **65,468**. The default value is **56** bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.
source ***source-address***	(Optional) Uses the source address that you specify, in the ping request packet.
strict	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.
strict-source [*hosts*]	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet, and uses the list of hosts you specify for routing the packet.
tos ***number***	(Optional) Sets the type-of-service (TOS) value in the IP header of the ping request packet. Specify a value from **0** through **255**.

Table 194: CLI ping Command Options *(continued)*

Option	Description
ttl *number*	(Optional) Sets the time-to-live (TTL) value for the ping request packet. Specify a value from **0** through **255**.
wait *seconds*	(Optional) Sets the maximum time to wait after sending the last ping request packet. If you do not specify this option, the default delay is **10** seconds. If you use this option without the **count** option, the device uses a default count of **5** packets.
detail	(Optional) Displays the interface on which the ping response was received.
verbose	(Optional) Displays detailed output.

The following is sample output from a **ping** command:

```
user@host> ping host3 count 4
```

```
PING host3.site.net (176.26.232.111): 56 data bytes 64 bytes from 176.26.232.111:
 icmp_seq=0 ttl=122 time=0.661 ms 64 bytes from 176.26.232.111: icmp_seq=1 ttl=122
 time=0.619 ms 64 bytes from 176.26.232.111: icmp_seq=2 ttl=122 time=0.621 ms 64
bytes from 176.26.232.111: icmp_seq=3 ttl=122 time=0.634 ms  --- host3.site.net
ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

The fields in the display are the same as those displayed by the J-Web ping host diagnostic tool.

RELATED DOCUMENTATION

Diagnostic Tools Overview | **16**

Understanding Ping MPLS | **1649**

Pinging Layer 2 Circuits | **1653**

Pinging Layer 2 VPNs | **1654**

Pinging Layer 3 VPNs | **1656**

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | **1657**

Interfaces User Guide for Security Devices

Pinging Layer 2 Circuits

Enter the **ping mpls l2circuit** command with the following syntax:

```
user@host> ping mpls l2circuit (interface interface-name | virtual-circuit neighbor prefix-name virtual-circuit-id)
  <exp forwarding-class> <count number> <source source-address> <detail>
```

Table 195 on page 1653 describes the **ping mpls l2circuit** command options.

Table 195: CLI ping mpls l2circuit Command Options

Option	Description
l2circuit interface ***interface-name***	Sends ping requests out the specified interface configured for the Layer 2 circuit on the outbound PE device.
l2circuit virtual-circuit neighbor ***prefix-name virtual-circuit-id***	Pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE device, testing the integrity of the Layer 2 circuit between the inbound and outbound PE devices.
exp ***forwarding-class***	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(Optional) Limits the number of ping requests to send. Specify a count from **0** through **1,000,000**. The default value is **5**. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
source ***source-address***	(Optional) Uses the source address that you specify, in the ping request packet.
detail	(Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.

To quit the **ping mpls l2circuit** command, press Ctrl-C.

The following is sample output from a **ping mpls l2circuit** command:

```
user@host> ping mpls l2circuit interface fe-1/0/0.0
```

```
Request for seq 1, to interface 69, labels <100000, 100208>
Reply for seq 1, return code: Egress-ok, time: 0.439 ms
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

RELATED DOCUMENTATION

- Using the ping Command | 1650
- Understanding Ping MPLS | 1649
- Pinging Layer 2 VPNs | 1654
- Pinging Layer 3 VPNs | 1656
- Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | 1657
- *Using the J-Web Ping Host Tool*

Pinging Layer 2 VPNs

Enter the **ping mpls l2vpn** command with the following syntax:

```
user@host> ping mpls l2vpn interface interface-name | instance l2vpn-instance-name local-site-id
  local-site-id-number remote-site-id remote-site-id-number <bottom-label-ttl> <exp forwarding-class>
  <count number> <source source-address> <detail>
```

Table 196 on page 1654 describes the **ping mpls l2vpn** command options.

Table 196: CLI ping mpls l2vpn Command Options

Option	Description
l2vpn interface ***interface-name***	Sends ping requests out the specified interface configured for the Layer 2 VPN on the outbound (egress) PE device.
l2vpn instance ***l2vpn-instance-name*** **local-site-id** ***local-site-id-number*** **remote-site-id** ***remote-site-id-number***	Pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, testing the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound (ingress) and outbound PE devices.
bottom-label-ttl	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
exp ***forwarding-class***	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(Optional) Limits the number of ping requests to send. Specify a count from **0** through **1,000,000**. The default value is **5**. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.

Table 196: CLI ping mpls l2vpn Command Options *(continued)*

Option	Description
source *source-address*	(Optional) Uses the source address that you specify, in the ping request packet.
detail	(Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.

To quit the **ping mpls l2vpn** command, press Ctrl-C.

The following is sample output from a **ping mpls l2vpn** command:

```
user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2 detail
```

```
Request for seq 1, to interface 68, labels <800001, 100176>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <800001, 100176>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <800001, 100176>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <800001, 100176>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <800001, 100176>
Reply for seq 5, return code: Egress-ok

--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

RELATED DOCUMENTATION

- Using the ping Command | **1650**
- Understanding Ping MPLS | **1649**
- Pinging Layer 2 Circuits | **1653**
- Pinging Layer 3 VPNs | **1656**
- Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | **1657**
- *Using the J-Web Ping Host Tool*

Pinging Layer 3 VPNs

Enter the **ping mpls l3vpn** command with the following syntax:

```
user@host> ping mpls l3vpn prefix prefix-name  <l3vpn-name> <bottom-label-ttl> <exp forwarding-class>
   <count number> <source source-address> <detail>
```

Table 197 on page 1656 describes the **ping mpls l3vpn** command options.

Table 197: CLI ping mpls l3vpn Command Options

Option	Description
l3vpn prefix *prefix-name*	Pings the remote host specified by the prefix to verify that the prefix is present in the PE device's VPN routing and forwarding (VRF) table. This option does not test the connectivity between a PE device and a CE device.
l3vpn-name	(Optional) Layer 3 VPN name.
bottom-label-ttl	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
exp *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(Optional) Limits the number of ping requests to send. Specify a count from **0** through **1,000,000**. The default value is **5**. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
source *source-address*	(Optional) Uses the source address that you specify, in the ping request packet.
detail	(Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.

To quit the **ping mpls l3vpn** command, press Ctrl-C.

The following is sample output from a **ping mpls l3vpn** command:

```
user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32
```

```
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

RELATED DOCUMENTATION

- Using the ping Command | 1650
- Understanding Ping MPLS | 1649
- Pinging Layer 2 Circuits | 1653
- Pinging Layer 2 VPNs | 1654
- Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs | 1657
- *Using the J-Web Ping Host Tool*

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs

Enter the **ping mpls** command with the following syntax:

```
user@host> ping mpls (ldp fec | lsp-end-point prefix-name | rsvp lsp-name) <exp forwarding-class> <count number>
  <source source-address> <detail>
```

Table 198 on page 1657 describes the **ping mpls** command options.

Table 198: CLI ping mpls ldp and ping mpls lsp-end-point Command Options

Option	Description
ldp ***fec***	Pings an LDP-signaled LSP identified by the forwarding equivalence class (FEC) prefix and length.
lsp-end-point ***prefix-name***	Pings an LSP endpoint using either an LDP FEC or a RSVP LSP endpoint address.
rsvp ***lsp-name***	Pings an RSVP-signaled LSP identified by the specified LSP name.

Table 198: CLI ping mpls ldp and ping mpls lsp-end-point Command Options *(continued)*

Option	Description
exp *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(Optional) Limits the number of ping requests to send. Specify a count from **0** through **1,000,000**. The default value is **5**. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
source *source-address*	(Optional) Uses the source address that you specify, in the ping request packet.
detail	(Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.

To quit the **ping mpls** command, press Ctrl-C.

The following is sample output from a **ping mpls** command:

```
user@host> ping mpls rsvp count 5
```

```
!!xxx
--- lsping statistics ---
5 packets transmitted, 2 packets received, 60% packet loss
3 packets received with error status, not counted as received.
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

RELATED DOCUMENTATION

Using the ping Command | **1650**

Understanding Ping MPLS | **1649**

Pinging Layer 2 Circuits | **1653**

Pinging Layer 2 VPNs | **1654**

Pinging Layer 3 VPNs | **1656**

Using the J-Web Ping Host Tool

CHAPTER 57

Using Packet Capture to Analyze Network Traffic

IN THIS CHAPTER

- Packet Capture Overview | 1659
- Example: Enabling Packet Capture on a Device | 1662
- Example: Configuring Packet Capture on an Interface | 1667
- Example: Configuring a Firewall Filter for Packet Capture | 1670
- Example: Configuring Packet Capture for Datapath Debugging | 1672
- Disabling Packet Capture | 1677
- Deleting Packet Capture Files | 1677
- Changing Encapsulation on Interfaces with Packet Capture Configured | 1679
- Displaying Packet Headers | 1680

Packet Capture Overview

IN THIS SECTION

- Packet Capture on Device Interfaces | 1660
- Firewall Filters for Packet Capture | 1661
- Packet Capture Files | 1661
- Analysis of Packet Capture Files | 1662

Packet capture is a tool that helps you to analyze network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets traveling over the network for monitoring and logging.

NOTE: Packet capture is supported on physical interfaces, reth interfaces, and tunnel interfaces, such as gr, ip, st0, and lsq-/ls.

Packets are captured as binary data, without modification. You can read the packet information offline with a packet analyzer such as Ethereal or tcpdump. If you need to quickly capture packets destined for, or originating from, the Routing Engine and analyze them online, you can use the J-Web packet capture diagnostic tool.

NOTE: The packet capture tool does not support IPv6 packet capture.

You can use either the J-Web configuration editor or CLI configuration editor to configure packet capture.

Network administrators and security engineers use packet capture to perform the following tasks:

- Monitor network traffic and analyze traffic patterns.
- Identify and troubleshoot network problems.
- Detect security breaches in the network, such as unauthorized intrusions, spyware activity, or ping scans.

Packet capture operates like traffic sampling on the device, except that it captures entire packets including the Layer 2 header and saves the contents to a file in libpcap format. Packet capture also captures IP fragments. You cannot enable packet capture and traffic sampling on the device at the same time. Unlike traffic sampling, there are no tracing operations for packet capture.

NOTE: You can enable packet capture and port mirroring simultaneously on a device.

This section contains the following topics:

Packet Capture on Device Interfaces

Packet capture is supported on the T1, T3, E1, E3, serial, Fast Ethernet, ADSL, G.SHDSL, PPPoE, and ISDN interfaces.

To capture packets on an ISDN interface, configure packet capture on the dialer interface. To capture packets on a PPPoE interface, configure packet capture on the PPPoE logical interface.

Packet capture supports PPP, Cisco HDLC, Frame Relay, and other ATM encapsulations. Packet capture also supports Multilink PPP (MLPPP), Multilink Frame Relay end-to-end (MLFR), and Multilink Frame Relay UNI/NNI (MFR) encapsulations.

You can capture all IPv4 packets flowing on an interface in the inbound or outbound direction. However, on traffic that bypasses the flow software module (protocol packets such as ARP, OSPF, and PIM), packets generated by the Routing Engine are not captured unless you have configured and applied a firewall filter on the interface in the outbound direction.

Tunnel interfaces can support packet capture in the outbound direction only.

Use the J-Web configuration editor or CLI configuration editor to specify the maximum packet size, the filename to be used for storing the captured packets, the maximum file size, the maximum number of packet capture files, and the file permissions.

> **NOTE:** For packets captured on T1, T3, E1, E3, serial, and ISDN interfaces in the outbound (egress) direction, the size of the packet captured might be 1 byte less than the maximum packet size configured because of the packet loss priority (PLP) bit.

To modify encapsulation on an interface that has packet capture configured, you must first disable packet capture.

Firewall Filters for Packet Capture

When you enable packet capture on a device, all packets flowing in the direction specified in packet capture configuration (inbound, outbound, or both) are captured and stored. Configuring an interface to capture all packets might degrade the performance of the device. You can control the number of packets captured on an interface with firewall filters and specify various criteria to capture packets for specific traffic flows.

You must also configure and apply appropriate firewall filters on the interface if you need to capture packets generated by the host device, because interface sampling does not capture packets originating from the host device.

Packet Capture Files

When packet capture is enabled on an interface, the entire packet including the Layer 2 header is captured and stored in a file. You can specify the maximum size of the packet to be captured, up to 1500 bytes. Packet capture creates one file for each physical interface. You can specify the target filename, the maximum size of the file, and the maximum number of files.

File creation and storage take place in the following way. Suppose you name the packet capture file **pcap-file**. Packet capture creates multiple files (one per physical interface), suffixing each file with the name of the physical interface; for example, **pcap-file.fe-0.0.1** for the Fast Ethernet interface **fe-0.0.1**.

When the file named **pcap-file.fe-0.0.1** reaches the maximum size, the file is renamed **pcap-file.fe-0.0.1.0**. When the file named **pcap-file.fe-0.0.1** reaches the maximum size again, the file named **pcap-file.fe-0.0.1.0** is renamed **pcap-file.fe-0.0.1.1** and **pcap-file.fe-0.0.1** is renamed **pcap-file.fe-0.0.1.0**. This process continues until the maximum number of files is exceeded and the oldest file is overwritten. The **pcap-file.fe-0.0.1** file is always the latest file.

Packet capture files are not removed even after you disable packet capture on an interface.

Analysis of Packet Capture Files

Packet capture files are stored in libpcap format in the **/var/tmp** directory. You can specify user or administrator privileges for the files.

Packet capture files can be opened and analyzed offline with tcpdump or any packet analyzer that recognizes the libpcap format. You can also use FTP or the Session Control Protocol (SCP) to transfer the packet capture files to an external device.

> **NOTE:** Disable packet capture before opening the file for analysis or transferring the file to an external device with FTP or SCP. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

RELATED DOCUMENTATION

Example: Enabling Packet Capture on a Device | **1662**

Example: Configuring Packet Capture on an Interface | **1667**

Example: Configuring a Firewall Filter for Packet Capture | **1670**

Using the J-Web Packet Capture Tool

Example: Enabling Packet Capture on a Device

IN THIS SECTION

- Requirements | **1663**
- Overview | **1663**

Configuration | 1663
Verification | 1665

This example shows how to enable packet capture on a device, allowing you to analyze network traffic and troubleshoot network problems

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See Interfaces User Guide for Security Devices.

Overview

In this example, you set the maximum packet capture size in each file as 500 bytes. The range is from 68 through 1500, and the default is 68 bytes. You specify the target filename for the packet capture file as pcap-file. You then specify the maximum number of files to capture as 100. The range is from 2 through 10,000, and the default is 10 files. You set the maximum size of each file to 1024 bytes. The range is from 1,024 through 104,857,600, and the default is 512,000 bytes. Finally, you specify that all users have permission to read the packet capture files.

Configuration

CLI Quick Configuration

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

```
set forwarding-options packet-capture maximum-capture-size 500
set forwarding-options packet-capture file filename pcap-file files 100 size 1024 world-readable
```

Step-by-Step Procedure

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

To enable packet capture on a device:

1. Set the maximum packet capture size.

```
[edit]
user@host# edit forwarding-options
user@host# set packet-capture maximum-capture-size 500
```

2. Specify the target filename.

```
[edit forwarding-options]
user@host# set packet-capture file filename pcap-file
```

3. Specify the maximum number of files to capture.

```
[edit forwarding-options]
user@host# set packet-capture file files 100
```

4. Specify the maximum size of each file.

```
[edit forwarding-options]
user@host# set packet-capture file size 1024
```

5. Specify that all users have permission to read the file.

```
[edit forwarding-options]
user@host# set packet-capture file world-readable
```

Results

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

```
[edit]
user@host# show forwarding-options
packet-capture {
```

```
    file filename pcap-file files 100 size 1k world-readable;
    maximum-capture-size 500;
}
```

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

Verification

IN THIS SECTION

- Verifying the Packet Capture Configuration | **1665**
- Verifying Captured Packets | **1665**

Confirm that the configuration is working properly.

Verifying the Packet Capture Configuration

Purpose

Verify that the packet capture is configured on the device.

Action

From configuration mode, enter the **show forwarding-options** command. Verify that the output shows the intended file configuration for capturing packets.

Verifying Captured Packets

Purpose

Verify that the packet capture file is stored under the **/var/tmp** directory and the packets can be analyzed offline.

Action

1. Disable packet capture.

   Using FTP, transfer a packet capture file (for example, **126b.fe-0.0.1**), to a server where you have installed packet analyzer tools (for example, **tools-server**).

   a. From configuration mode, connect to **tools-server** using FTP.

```
[edit]
user@host# run ftp tools-server
Connected to tools-server.mydomain.net
```

```
220 tools-server.mydomain.net FTP server (Version 6.00LS) ready
Name (tools-server:user):remoteuser
331 Password required for remoteuser.
Password:
230 User remoteuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

b. Navigate to the directory where packet capture files are stored on the device.

```
ftp> lcd /var/tmp
Local directory now /cf/var/tmp
```

c. Copy the packet capture file that you want to analyze to the server, for example **126b.fe-0.0.1**.

```
ftp> put 126b.fe-0.0.1
local: 126b.fe-0.0.1 remote: 126b.fe-0.0.1
200 PORT command successful.
150 Opening BINARY mode data connection for '126b.fe-0.0.1'.
100% 1476 00:00 ETA
226 Transfer complete.
1476 bytes sent in 0.01 seconds (142.42 KB/s)
```

d. Return to configuration mode.

```
ftp> bye
221 Goodbye.
[edit]
user@host#
```

2. Open the packet capture file on the server with tcpdump or any packet analyzer that supports libpcap format and review the output.

```
root@server% tcpdump -r 126b.fe-0.0.1 -xevvvv
```

```
01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl  64, id 33133, offset 0, flags [none], proto: ICMP (1),
```

```
length: 84) 14.1.1.1 > 15.1.1.1: ICMP echo request seq 0, length 64
                         0005 85c8 f6d1 0005 85c4 e3d1 0800 4500
                         0054 816d 0000 4001 da38 0e01 0101 0f01
                         0101 0800 3c5a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
01:12:36.279793 Out 0:5:85:c8:f6:d1 > 0:5:85:c4:e3:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl  63, id 41227, offset 0, flags [none], proto: ICMP (1),
length: 84) 15.1.1.1 > 14.1.1.1: ICMP echo reply seq 0, length 64
                         0005 85c4 e3d1 0005 85c8 f6d1 0800 4500
                         0054 a10b 0000 3f01 bb9a 0f01 0101 0e01
                         0101 0000 445a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
root@server%
```

RELATED DOCUMENTATION

- Packet Capture Overview | **1659**
- Example: Configuring Packet Capture on an Interface | **1667**
- Example: Configuring a Firewall Filter for Packet Capture | **1670**
- Disabling Packet Capture | **1677**
- Deleting Packet Capture Files | **1677**
- Disabling Packet Capture | **1677**

Example: Configuring Packet Capture on an Interface

IN THIS SECTION

- Requirements | **1668**
- Overview | **1668**

Configuration | 1668
Verification | 1669

This example shows how to configure packet capture on an interface to analyze traffic.

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See Interfaces User Guide for Security Devices.

Overview

In this example, you create an interface called fe-0/0/1. You then configure the direction of the traffic for which you are enabling packet capture on the logical interface as inbound and outbound.

> **NOTE:** On traffic that bypasses the flow software module (protocol packets such as ARP, OSPF, and PIM), packets generated by the Routing Engine are not captured unless you have configured and applied a firewall filter on the interface in the output direction.

Configuration

CLI Quick Configuration

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

```
edit interfaces fe-0/0/1
set unit 0 family inet sampling input output
```

Step-by-Step Procedure

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

To configure packet capture on an interface:

1. Create an interface.

```
[edit]
user@host# edit interfaces fe-0/0/1
```

2. Configure the direction of the traffic.

```
[edit interfaces fe-0/0/1]
user@host# set unit 0 family inet sampling input output
```

3. If you are done configuring the device, commit the configuration.

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

Verification

Verifying the Packet Capture Configuration

Purpose

Confirm that the configuration is working properly.

Verify that packet capture is configured on the interface.

Action

From configuration mode, enter the **show interfaces fe-0/0/1** command.

RELATED DOCUMENTATION

- Packet Capture Overview | **1659**
- Changing Encapsulation on Interfaces with Packet Capture Configured | **1679**
- Example: Configuring a Firewall Filter for Packet Capture | **1670**
- Example: Enabling Packet Capture on a Device | **1662**
- Deleting Packet Capture Files | **1677**

Disabling Packet Capture | 1677

Example: Configuring a Firewall Filter for Packet Capture

IN THIS SECTION

- Requirements | 1670
- Overview | 1670
- Configuration | 1670
- Verification | 1672

This example shows how to configure a firewall filter for packet capture and apply it to a logical interface.

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See Interfaces User Guide for Security Devices.

Overview

In this example, you set a firewall filter called dest-all and a term name called dest-term to capture packets from a specific destination address, which is 192.168.1.1/32. You define the match condition to accept the sampled packets. Finally, you apply the dest-all filter to all of the outgoing packets on interface fe-0/0/1.

> **NOTE:** If you apply a firewall filter on the loopback interface, it affects all traffic to and from the Routing Engine. If the firewall filter has a **sample** action, packets to and from the Routing Engine are sampled. If packet capture is enabled, then packets to and from the Routing Engine are captured in the files created for the input and output interfaces.

Configuration

CLI Quick Configuration

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

```
set firewall filter dest-all term dest-term from destination-address 192.168.1.1/32
set firewall filter dest-all term dest-term then sample accept
edit interfaces
set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

Step-by-Step Procedure

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

To configure a firewall filter for packet capture and apply it to a logical interface:

1. Specify the firewall filter and its destination address.

```
[edit]
user@host# edit firewall
user@host# set filter dest-all term dest-term from destination-address 192.168.1.1/32
```

2. Define the match condition and its action.

```
[edit firewall]
user@host# set filter dest-all term dest-term then sample accept
```

3. Apply the filter to all the outgoing packets.

```
[edit interfaces]
user@host# set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

Results

From configuration mode, confirm your configuration by entering the **show firewall filter dest-all** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show firewall filter dest-all
term dest-term {
   from {
```

```
        destination-address 192.168.1.1/32;
    }
    then {
        sample;
        accept;
    }
}
```

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

Verification

Verifying the Firewall Filter for Packet Capture Configuration

Purpose

Confirm that the configuration is working properly.

Verify that the firewall filter for packet capture is configured.

Action

From configuration mode, enter the **show firewall filter dest-all** command. Verify that the output shows the intended configuration of the firewall filter for capturing packets sent to the destination address.

RELATED DOCUMENTATION

- Packet Capture Overview | **1659**
- Example: Configuring Packet Capture on an Interface | **1667**
- Example: Enabling Packet Capture on a Device | **1662**
- Deleting Packet Capture Files | **1677**
- Disabling Packet Capture | **1677**

Example: Configuring Packet Capture for Datapath Debugging

IN THIS SECTION

- Requirements | **1673**
- Overview | **1673**

Configuration | **1673**
Verification | **1676**

This example shows how to configure packet capture to monitor traffic that passes through the device. Packet capture then dumps the packets into a PCAP file format that can be later examined by the tcpdump utility.

Requirements

Before you begin, see "Debugging the Data Path (CLI Procedure)" on page 1631.

Overview

A filter is defined to filter traffic; then an action profile is applied to the filtered traffic. The action profile specifies a variety of actions on the processing unit. One of the supported actions is packet dump, which sends the packet to the Routing Engine and stores it in proprietary form to be read using the **show security datapath-debug capture** command.

> **NOTE:** Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

Configuration

CLI Quick Configuration

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

```
set security datapath-debug capture-file my-capture
set security datapath-debug capture-file format pcap
set security datapath-debug capture-file size 1m
set security datapath-debug capture-file files 5
set security datapath-debug maximum-capture-size 400
set security datapath-debug action-profile do-capture event np-ingress packet-dump
set security datapath-debug packet-filter my-filter action-profile do-capture
set security datapath-debug packet-filter my-filter source-prefix 1.2.3.4/32
```

Step-by-Step Procedure

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

To configure packet capture:

1. Edit the security datapath-debug option for the multiple processing units along the packet-processing path:

```
[edit]
user@host# edit security datapath-debug
```

2. Enable the capture file, the file format, the file size, and the number of files. Size number limits the size of the capture file. After the limit size is reached, if the file number is specified, then the capture file will be rotated to filename *x*, where *x* is auto-incremented until it reaches the specified index and then returns to zero. If no files index is specified, the packets will be discarded after the size limit is reached. The default size is 512 kilobytes.

```
[edit security datapath-debug]
user@host# set capture-file my-capture format pcap size 1m files 5
[edit security datapath-debug]
user@host# set maximum-capture-size 400
```

3. Enable action profile and set the event. Set the action profile as do-capture and the event type as np-ingress:

```
[edit security datapath-debug]
user@host# edit action-profile do-capture
[edit security datapath-debug action-profile do-capture]
user@host# edit event np-ingress
```

4. Enable packet dump for the action profile:

```
[edit security datapath-debug action-profile do-capture event np-ingress]
user@host# set packet-dump
```

5. Enable packet filter, action, and filter options. The packet filter is set to my-filter, the action profile is set to do-capture, and filter option is set to source-prefix 1.2.3.4/32.

```
[edit security datapath-debug]
```

```
user@host# set security datapath-debug packet-filter my-filter action-profile do-capture
```

```
[edit security datapath-debug]
user@host#  set security datapath-debug packet-filter my-filter source-prefix 1.2.3.4/32
```

Results

From configuration mode, confirm your configuration by entering the **show security datapath-debug** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it. The following is**show security datapath-debug** output from the **show security datapath-debug** command:

```
security {
    datapath-debug {
        capture-file {
            my-capture
            format pcap
            size 1m
            files 5;
        }
    }
    maximum-capture-size 100;
    action-profile do-capture {
        event np-ingress {
            packet-dump
        }
    }
    packet-filter my-filter {
        source-prefix 1.2.3.4/32
        action-profile do-capture
    }
}
```

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

Verification

IN THIS SECTION

- Verifying Packet Capture | 1676
- Verifying Data Path Debugging Capture | 1676
- Verifying Data Path Debugging Counter | 1677

Confirm that the configuration is working properly.

Verifying Packet Capture

Purpose

Verify if the packet capture is working.

Action

From operational mode, enter the **request security datapath-debug capture start** command to start packet capture and enter the **request security datapath-debug capture stop** command to stop packet capture.

To view the results, from CLI operational mode, access the local UNIX shell and navigate to the directory /var/log/my-capture. The result can be read by using the tcpdump utility.

Verifying Data Path Debugging Capture

Purpose

Verify the details of data path debugging capture file.

Action

From operational mode, enter the **show security datapath-debug capture** command.

```
user@host>show security datapath-debug capture
```

WARNING: When you are done troubleshooting, make sure to remove or deactivate all the traceoptions configurations (not limited to flow traceoptions) and the complete security datapath-debug configuration stanza. If any debugging configurations remain active, they will continue to use the device's CPU and memory resources.

Verifying Data Path Debugging Counter

Purpose

Verify the details of the data path debugging counter.

Action

From operational mode, enter the **show security datapath-debug counter** command.

Disabling Packet Capture

You must disable packet capture before opening the packet capture file for analysis or transferring the file to an external device. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

To disable packet capture, enter from configuration mode:

```
[edit forwarding-options]
user@host# set packet-capture disable
```

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

RELATED DOCUMENTATION

- Packet Capture Overview | 1659
- Example: Configuring Packet Capture on an Interface | 1667
- Example: Configuring a Firewall Filter for Packet Capture | 1670
- Example: Enabling Packet Capture on a Device | 1662
- Deleting Packet Capture Files | 1677

Deleting Packet Capture Files

Deleting packet capture files from the /var/tmp directory only temporarily removes the packet capture files. Packet capture files for the interface are automatically created again the next time a packet capture configuration change is committed or as part of a packet capture file rotation.

To delete a packet capture file:

1. Disable packet capture (see "Disabling Packet Capture" on page 1677).

2. Delete the packet capture file for the interface.

   a. From operational mode, access the local UNIX shell.

   ```
   user@host> start shell
   %
   ```

   b. Navigate to the directory where packet capture files are stored.

   ```
   % cd /var/tmp
   %
   ```

   c. Delete the packet capture file for the interface; for example **pcap-file.fe.0.0.0**.

   ```
   % rm pcap-file.fe.0.0.0
   %
   ```

   d. Return to operational mode.

   ```
   % exit
   user@host>
   ```

3. Reenable packet capture (see "Example: Enabling Packet Capture on a Device" on page 1662).

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

RELATED DOCUMENTATION

- Packet Capture Overview | 1659
- Example: Configuring Packet Capture on an Interface | 1667
- Example: Configuring a Firewall Filter for Packet Capture | 1670
- Example: Enabling Packet Capture on a Device | 1662
- Changing Encapsulation on Interfaces with Packet Capture Configured | 1679
- Disabling Packet Capture | 1677

Changing Encapsulation on Interfaces with Packet Capture Configured

Before modifying the encapsulation on a device interface that is configured for packet capture, you must disable packet capture and rename the latest packet capture file. Otherwise, packet capture saves the packets with different encapsulations in the same packet capture file. Packet files containing packets with different encapsulations are not useful, because packet analyzer tools like tcpdump cannot analyze such files.

After modifying the encapsulation, you can safely reenable packet capture on the device.

To change the encapsulation on interfaces with packet capture configured:

1. Disable packet capture (see "Disabling Packet Capture" on page 1677).

2. Enter **commit** from configuration mode.

3. Rename the latest packet capture file on which you are changing the encapsulation with the **.chdsl** extension.

   a. From operational mode, access the local UNIX shell.

   ```
   user@host> start shell
   %
   ```

   b. Navigate to the directory where packet capture files are stored.

   ```
   % cd /var/tmp
   %
   ```

   c. Rename the latest packet capture file for the interface on which you are changing the encapsulation; for example **fe.0.0.0**.

   ```
   % mv pcap-file.fe.0.0.0 pcap-file.fe.0.0.0.chdsl
   %
   ```

   d. Return to operational mode.

   ```
   % exit
   user@host>
   ```

4. Change the encapsulation on the interface using the J-Web user interface or CLI configuration editor.

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

6. Reenable packet capture (see "Example: Enabling Packet Capture on a Device" on page 1662).

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

RELATED DOCUMENTATION

Packet Capture Overview | 1659

Example: Configuring Packet Capture on an Interface | 1667

Example: Configuring a Firewall Filter for Packet Capture | 1670

Example: Enabling Packet Capture on a Device | 1662

Displaying Packet Headers

Enter the **monitor traffic** command to display packet headers transmitted through network interfaces with the following syntax:

> **NOTE:** Using the **monitor traffic** command can degrade system performance. We recommend that you use filtering options—such as **count** and **matching**—to minimize the impact to packet throughput on the system.

```
user@host> monitor traffic <absolute-sequence> <count number> <interface interface-name> <layer2-headers>
  <matching "expression"> <no-domain-names> <no-promiscuous> <no-resolve> <no-timestamp> <print-ascii>
  <print-hex> <size bytes> <brief | detail | extensive>
```

Table 199 on page 1680 describes the **monitor traffic** command options.

Table 199: CLI monitor traffic Command Options

Option	Description
absolute-sequence	(Optional) Displays the absolute TCP sequence numbers.
count *number*	(Optional) Displays the specified number of packet headers. Specify a value from **0** through **100,000**. The command quits and exits to the command prompt after this number is reached.

Table 199: CLI monitor traffic Command Options *(continued)*

Option	Description
interface *interface-name*	(Optional) Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.
layer2-headers	(Optional) Displays the link-layer packet header on each line.
matching "*expression*"	(Optional) Displays packet headers that match an expression enclosed in quotation marks (" "). Table 200 on page 1682 through Table 202 on page 1685 list match conditions, logical operators, and arithmetic, binary, and relational operators you can use in the expression.
no-domain-names	(Optional) Suppresses the display of the domain name portion of the hostname.
no-promiscuous	(Optional) Specifies *not* to place the monitored interface in promiscuous mode. In promiscuous mode, the interface reads every packet that reaches it. In nonpromiscuous mode, the interface reads only the packets addressed to it.
no-resolve	(Optional) Suppresses the display of hostnames.
no-timestamp	(Optional) Suppresses the display of packet header timestamps.
print-ascii	(Optional) Displays each packet header in ASCII format.
print-hex	(Optional) Displays each packet header, except link-layer headers, in hexadecimal format.
size *bytes*	(Optional) Displays the number of bytes for each packet that you specify. If a packet header exceeds this size, the displayed packet header is truncated. The default value is **96**.
brief	(Optional) Displays minimum packet header information. This is the default.
detail	(Optional) Displays packet header information in moderate detail. For some protocols, you must also use the **size** option to see detailed information.

Table 199: CLI monitor traffic Command Options *(continued)*

Option	Description
extensive	(Optional) Displays the most extensive level of packet header information. For some protocols, you must also use the **size** option to see extensive information.

To quit the **monitor traffic** command and return to the command prompt, press Ctrl-C.

To limit the packet header information displayed by the **monitor traffic** command, include the **matching "*expression*"** option. An expression consists of one or more match conditions listed in Table 200 on page 1682, enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in Table 201 on page 1684 (shown in order of highest to lowest precedence).

For example, to display TCP or UDP packet headers, enter:

```
user@host> monitor traffic matching “tcp || udp”
```

To compare the following types of expressions, use the relational operators listed in Table 202 on page 1685 (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in Table 202 on page 1685.
- Binary—Expressions that use the binary operators listed in Table 202 on page 1685.
- Packet data accessor—Expressions that use the following syntax:

  ```
  protocol [byte-offset <size>]
  ```

  Replace ***protocol*** with any protocol in Table 200 on page 1682. Replace ***byte-offset*** with the byte offset, from the beginning of the packet header, to use for the comparison. The optional ***size*** parameter represents the number of bytes examined in the packet header—1, 2, or 4 bytes.

  For example, the following command displays all multicast traffic:

  ```
  user@host> monitor traffic matching “ether[0] & 1 !=0”
  ```

Table 200: CLI monitor traffic Match Conditions

Match Condition	Description
Entity Type	

Table 200: CLI monitor traffic Match Conditions *(continued)*

Match Condition	Description
host [*address* | *hostname*]	Matches packet headers that contain the specified address or hostname. You can preprend any of the following protocol match conditions, followed by a space, to **host**: **arp**, **ip**, **rarp**, or any of the Directional match conditions.
network *address*	Matches packet headers with source or destination addresses containing the specified network address.
network *address* mask *mask*	Matches packet headers containing the specified network address and subnet mask.
port [*port-number* | *port-name*]	Matches packet headers containing the specified source or destination TCP or UDP port number or port name.
Directional	
destination	Matches packet headers containing the specified destination. Directional match conditions can be prepended to any Entity Type match conditions, followed by a space.
source	Matches packet headers containing the specified source.
source and destination	Matches packet headers containing the specified source *and* destination.
source or destination	Matches packet headers containing the specified source *or* destination.
Packet Length	
less *bytes*	Matches packets with lengths less than or equal to the specified value, in bytes.
greater *bytes*	Matches packets with lengths greater than or equal to the specified value, in bytes.
Protocol	
arp	Matches all ARP packets.
ether	Matches all Ethernet frames.
ether [broadcast | multicast]	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with **source** or **destination**.

Table 200: CLI monitor traffic Match Conditions *(continued)*

Match Condition	Description
ether protocol [*address* | (\arp | \ip | \rarp)	Matches Ethernet frames with the specified address or protocol type. The arguments **arp**, **ip**, and **rarp** are also independent match conditions, so they must be preceded with a backslash (\) when used in the **ether protocol** match condition.
icmp	Matches all ICMP packets.
ip	Matches all IP packets.
ip [broadcast | multicast]	Matches broadcast or multicast IP packets.
ip protocol [*address* | (\icmp | igrp | \tcp | \udp)]	Matches IP packets with the specified address or protocol type. The arguments **icmp**, **tcp**, and **udp** are also independent match conditions, so they must be preceded with a backslash (\) when used in the **ip protocol** match condition.
isis	Matches all IS-IS routing messages.
rarp	Matches all RARP packets.
tcp	Matches all TCP packets.
udp	Matches all UDP packets.

Table 201: CLI monitor traffic Logical Operators

Logical Operator	Description
!	Logical NOT. If the first condition does not match, the next condition is evaluated.
&&	Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.
||	Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.
()	Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).

Table 202: CLI monitor traffic Arithmetic, Binary, and Relational Operators

Operator	Description
Arithmetic Operator	
+	Addition operator.
–	Subtraction operator.
/	Division operator.
Binary Operator	
&	Bitwise AND.
*	Bitwise exclusive OR.
|	Bitwise inclusive OR.
Relational Operator	
<=	A match occurs if the first expression is less than or equal to the second.
>=	A match occurs if the first expression is greater than or equal to the second.
<	A match occurs if the first expression is less than the second.
>	A match occurs if the first expression is greater than the second.
=	A match occurs if the first expression is equal to the second.
!=	A match occurs if the first expression is not equal to the second.

The following is sample output from the **monitor traffic** command:

```
user@host> monitor traffic count 4 matching “arp” detail
```

```
Listening on fe-0/0/0, capture size 96 bytes  15:04:16.276780  In arp who-has
193.1.1.1 tell host1.site2.net 15:04:16.376848  In arp who-has host2.site2.net
tell host1.site2.net 15:04:16.376887  In arp who-has 193.1.1.2 tell host1.site2.net
 15:04:16.601923  In arp who-has 193.1.1.3 tell host1.site2.net
```

RELATED DOCUMENTATION

Packet Capture Overview | 1659

Using the J-Web Packet Capture Tool

Changing Encapsulation on Interfaces with Packet Capture Configured | 1679

Example: Configuring Packet Capture on an Interface | 1667

CHAPTER 58

Troubleshooting Security Devices

IN THIS CHAPTER

- Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only) | 1687
- Troubleshooting the Link Services Interface | 1688
- Troubleshooting Security Policies | 1700
- Log Error Messages used for Troubleshooting ISSU-Related Problems | 1702

Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)

Problem

Description: The address of a hostname in an address book entry that is used in a security policy might fail to resolve correctly.

Cause

Normally, address book entries that contain dynamic hostnames refresh automatically for SRX Series devices. The TTL field associated with a DNS entry indicates the time after which the entry should be refreshed in the policy cache. Once the TTL value expires, the SRX Series device automatically refreshes the DNS entry for an address book entry.

However, if the SRX Series device is unable to obtain a response from the DNS server (for example, the DNS request or response packet is lost in the network or the DNS server cannot send a response), the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found.

Solution

The master administrator can use the **show security dns-cache** command to display DNS cache information on the SRX Series device. If the DNS cache information needs to be refreshed, the master administrator can use the **clear security dns-cache** command.

NOTE: These commands are only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

RELATED DOCUMENTATION

Understanding Logical Systems Security Policies

Troubleshooting the Link Services Interface

IN THIS SECTION

- Determine Which CoS Components Are Applied to the Constituent Links | **1688**
- Determine What Causes Jitter and Latency on the Multilink Bundle | **1690**
- Determine If LFI and Load Balancing Are Working Correctly | **1691**
- Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device | **1699**

To solve configuration problems on a link services interface:

Determine Which CoS Components Are Applied to the Constituent Links

Problem

Description: You are configuring a multilink bundle, but you also have traffic without MLPPP encapsulation passing through constituent links of the multilink bundle. Do you apply all CoS components to the constituent links, or is applying them to the multilink bundle enough?

Solution

You can apply a scheduler map to the multilink bundle and its constituent links. Although you can apply several CoS components with the scheduler map, configure only the ones that are required. We recommend that you keep the configuration on the constituent links simple to avoid unnecessary delay in transmission.

Table 203 on page 1689 shows the CoS components to be applied on a multilink bundle and its constituent links.

Table 203: CoS Components Applied on Multilink Bundles and Constituent Links

Cos Component	Multilink Bundle	Constituent Links	Explanation
Classifier	Yes	No	CoS classification takes place on the incoming side of the interface, not on the transmitting side, so no classifiers are needed on constituent links.
Forwarding class	Yes	No	Forwarding class is associated with a queue, and the queue is applied to the interface by a scheduler map. The queue assignment is predetermined on the constituent links. All packets from Q2 of the multilink bundle are assigned to Q2 of the constituent link, and packets from all the other queues are queued to Q0 of the constituent link.
Scheduler map	Yes	Yes	Apply scheduler maps on the multilink bundle and the constituent link as follows: • Transmit rate—Make sure that the relative order of the transmit rate configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle. • Scheduler priority—Make sure that the relative order of the scheduler priority configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle. • Buffer size—Because all non-LFI packets from the multilink bundle transit on Q0 of the constituent links, make sure that the buffer size on Q0 of the constituent links is large enough. • RED drop profile—Configure a RED drop profile on the multilink bundle only. Configuring the RED drop profile on the constituent links applies a back pressure mechanism that changes the buffer size and introduces variation. Because this behavior might cause fragment drops on the constituent links, make sure to leave the RED drop profile at the default settings on the constituent links.

Table 203: CoS Components Applied on Multilink Bundles and Constituent Links *(continued)*

Cos Component	Multilink Bundle	Constituent Links	Explanation
Shaping rate for a per-unit scheduler or an interface-level scheduler	No	Yes	Because per-unit scheduling is applied only at the end point, apply this shaping rate to the constituent links only. Any configuration applied earlier is overwritten by the constituent link configuration.
Transmit-rate exact or queue-level shaping	Yes	No	The interface-level shaping applied on the constituent links overrides any shaping on the queue. Thus apply transmit-rate exact shaping on the multilink bundle only.
Rewrite rules	Yes	No	Rewrite bits are copied from the packet into the fragments automatically during fragmentation. Thus what you configure on the multilink bundle is carried on the fragments to the constituent links.
Virtual channel group	Yes	No	Virtual channel groups are identified through firewall filter rules that are applied on packets only before the multilink bundle. Thus you do not need to apply the virtual channel group configuration to the constituent links.

SEE ALSO

See the *Junos OS Class of Service Configuration Guide for Security Devices*

Determine What Causes Jitter and Latency on the Multilink Bundle

Problem

Description: To test jitter and latency, you send three streams of IP packets. All packets have the same IP precedence settings. After configuring LFI and CRTP, the latency increased even over a noncongested link. How can you reduce jitter and latency?

Solution

To reduce jitter and latency, do the following:

1. Make sure that you have configured a shaping rate on each constituent link.

2. Make sure that you have not configured a shaping rate on the link services interface.

3. Make sure that the configured shaping rate value is equal to the physical interface bandwidth.

4. If shaping rates are configured correctly, and jitter still persists, contact the Juniper Networks Technical Assistance Center (JTAC).

SEE ALSO

RPM Overview

Determine If LFI and Load Balancing Are Working Correctly

Problem

Description: In this case, you have a single network that supports multiple services. The network transmits data and delay-sensitive voice traffic. After configuring MLPPP and LFI, make sure that voice packets are transmitted across the network with very little delay and jitter. How can you find out if voice packets are being treated as LFI packets and load balancing is performed correctly?

Solution

When LFI is enabled, data (non-LFI) packets are encapsulated with an MLPPP header and fragmented to packets of a specified size. The delay-sensitive, voice (LFI) packets are PPP-encapsulated and interleaved between data packet fragments. Queuing and load balancing are performed differently for LFI and non-LFI packets.

To verify that LFI is performed correctly, determine that packets are fragmented and encapsulated as configured. After you know whether a packet is treated as an LFI packet or a non-LFI packet, you can confirm whether the load balancing is performed correctly.

Solution Scenario—Suppose two Juniper Networks devices, R0 and R1, are connected by a multilink bundle **lsq-0/0/0.0** that aggregates two serial links, **se-1/0/0** and **se-1/0/1**. On R0 and R1, MLPPP and LFI are enabled on the link services interface and the fragmentation threshold is set to 128 bytes.

In this example, we used a packet generator to generate voice and data streams. You can use the packet capture feature to capture and analyze the packets on the incoming interface.

The following two data streams were sent on the multilink bundle:

- 100 data packets of 200 bytes (larger than the fragmentation threshold)
- 500 data packets of 60 bytes (smaller than the fragmentation threshold)

The following two voice streams were sent on the multilink bundle:

- 100 voice packets of 200 bytes from source port 100
- 300 voice packets of 200 bytes from source port 200

To confirm that LFI and load balancing are performed correctly:

> **NOTE:** Only the significant portions of command output are displayed and described in this example.

1. Verify packet fragmentation. From operational mode, enter the **show interfaces lsq-0/0/0** command to check that large packets are fragmented correctly.

   `user@R0#>` **show interfaces lsq-0/0/0**

```
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2006-08-01 10:45:13 PDT (2w0d 06:06 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

  Logical interface lsq-0/0/0.0 (Index 69) (SNMP ifIndex 42)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
    Bandwidth: 16mbps
    Statistics         Frames      fps       Bytes        bps
    Bundle:
      Fragments:
        Input :             0        0           0          0
        Output:          1100        0      118800          0
      Packets:
        Input :             0        0           0          0
        Output:          1000        0      112000          0
   ...
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 9.9.9/24, Local: 9.9.9.10
```

Meaning—The output shows a summary of packets transiting the device on the multilink bundle. Verify the following information on the multilink bundle:

- The total number of transiting packets = 1000
- The total number of transiting fragments=1100
- The number of data packets that were fragmented =100

The total number of packets sent (600 + 400) on the multilink bundle match the number of transiting packets (1000), indicating that no packets were dropped.

The number of transiting fragments exceeds the number of transiting packets by 100, indicating that 100 large data packets were correctly fragmented.

Corrective Action—If the packets are not fragmented correctly, check your fragmentation threshold configuration. Packets smaller than the specified fragmentation threshold are not fragmented.

2. Verify packet encapsulation. To find out whether a packet is treated as an LFI or non-LFI packet, determine its encapsulation type. LFI packets are PPP encapsulated, and non-LFI packets are encapsulated with both PPP and MLPPP. PPP and MLPPP encapsulations have different overheads resulting in different-sized packets. You can compare packet sizes to determine the encapsulation type.

   A small unfragmented data packet contains a PPP header and a single MLPPP header. In a large fragmented data packet, the first fragment contains a PPP header and an MLPPP header, but the consecutive fragments contain only an MLPPP header.

   PPP and MLPPP encapsulations add the following number of bytes to a packet:

   - PPP encapsulation adds 7 bytes:

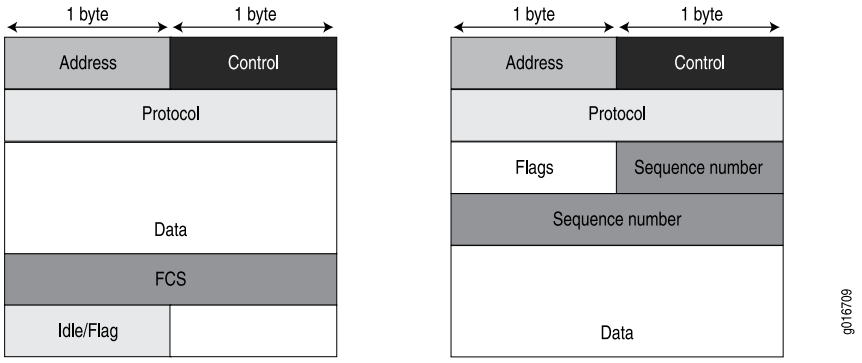
     4 bytes of header+2 bytes of frame check sequence (FCS)+1 byte that is idle or contains a flag

   - MLPPP encapsulation adds between 6 and 8 bytes:

     4 bytes of PPP header+2 to 4 bytes of multilink header

   Figure 57 on page 1694 shows the overhead added to PPP and MLPPP headers.

Figure 57: PPP and MLPPP Headers



   For CRTP packets, the encapsulation overhead and packet size are even smaller than for an LFI packet. For more information, see Example: Configuring the Compressed Real-Time Transport Protocol.

   Table 204 on page 1694 shows the encapsulation overhead for a data packet and a voice packet of 70 bytes each. After encapsulation, the size of the data packet is larger than the size of the voice packet.

Table 204: PPP and MLPPP Encapsulation Overhead

Packet Type	Encapsulation	Initial Packet Size	Encapsulation Overhead	Packet Size after Encapsulation
Voice packet (LFI)	PPP	70 bytes	4 + 2 + 1 = 7 bytes	77 bytes

Table 204: PPP and MLPPP Encapsulation Overhead *(continued)*

Packet Type	Encapsulation	Initial Packet Size	Encapsulation Overhead	Packet Size after Encapsulation
Data fragment (non-LFI) with short sequence	MLPPP	70 bytes	4 + 2 + 1 + 4 + 2 = 13 bytes	83 bytes
Data fragment (non-LFI) with long sequence	MLPPP	70 bytes	4 + 2 + 1 + 4 + 4 = 15 bytes	85 bytes

From operational mode, enter the **show interfaces queue** command to display the size of transmitted packet on each queue. Divide the number of bytes transmitted by the number of packets to obtain the size of the packets and determine the encapsulation type.

3. Verify load balancing. From operational mode, enter the **show interfaces queue** command on the multilink bundle and its constituent links to confirm whether load balancing is performed accordingly on the packets.

```
user@R0> show interfaces queue lsq-0/0/0
```

```
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :               600                 0 pps
    Bytes                :             44800                 0 bps
  Transmitted:
    Packets              :               600                 0 pps
    Bytes                :             44800                 0 bps
    Tail-dropped packets :                 0                 0 pps
    RED-dropped packets  :                 0                 0 pps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                 0                 0 pps
    Bytes                :                 0                 0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :               400                 0 pps
```

```
    Bytes               :             61344                 0 bps
  Transmitted:
    Packets             :               400                 0 pps
    Bytes               :             61344                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets             :                 0                 0 pps
    Bytes               :                 0                 0 bps
 …
```

user@R0> **show interfaces queue se-1/0/0**

```
Physical interface: se-1/0/0, Enabled, Physical link is Up
  Interface index: 141, SNMP ifIndex: 35
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets             :               350                 0 pps
    Bytes               :             24350                 0 bps
  Transmitted:
    Packets             :               350                 0 pps
    Bytes               :             24350                 0 bps
   ...
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets             :                 0                 0 pps
    Bytes               :                 0                 0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets             :               100                 0 pps
    Bytes               :             15272                 0 bps
  Transmitted:
    Packets             :               100                 0 pps
    Bytes               :             15272                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets             :                19                 0 pps
    Bytes               :               247                 0 bps
  Transmitted:
    Packets             :                19                 0 pps
```

```
    Bytes                :                247                0 bps
    …
```

`user@R0>` **show interfaces queue se-1/0/1**

```
Physical interface: se-1/0/1, Enabled, Physical link is Up
  Interface index: 142, SNMP ifIndex: 38
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                350                0 pps
    Bytes                :              24350                0 bps
  Transmitted:
    Packets              :                350                0 pps
    Bytes                :              24350                0 bps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                0 pps
    Bytes                :                  0                0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                300                0 pps
    Bytes                :              45672                0 bps
  Transmitted:
    Packets              :                300                0 pps
    Bytes                :              45672                0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                 18                0 pps
    Bytes                :                234                0 bps
  Transmitted:
    Packets              :                 18                0 pps
    Bytes                :                234                0 bps
```

Meaning—The output from these commands shows the packets transmitted and queued on each queue of the link services interface and its constituent links. Table 205 on page 1698 shows a summary of these values. (Because the number of transmitted packets equaled the number of queued packets on all the links, this table shows only the queued packets.)

Table 205: Number of Packets Transmitted on a Queue

Packets Queued	Bundle lsq-0/0/0.0	Constituent Link se-1/0/0	Constituent Link se-1/0/1	Explanation
Packets on Q0	600	350	350	The total number of packets transiting the constituent links (350+350 = 700) exceeded the number of packets queued (600) on the multilink bundle.
Packets on Q2	400	100	300	The total number of packets transiting the constituent links equaled the number of packets on the bundle.
Packets on Q3	0	19	18	The packets transiting Q3 of the constituent links are for keepalive messages exchanged between constituent links. Thus no packets were counted on Q3 of the bundle.

On the multilink bundle, verify the following:

- The number of packets queued matches the number transmitted. If the numbers match, no packets were dropped. If more packets were queued than were transmitted, packets were dropped because the buffer was too small. The buffer size on the constituent links controls congestion at the output stage. To correct this problem, increase the buffer size on the constituent links.
- The number of packets transiting Q0 (600) matches the number of large and small data packets received (100+500) on the multilink bundle. If the numbers match, all data packets correctly transited Q0.
- The number of packets transiting Q2 on the multilink bundle (400) matches the number of voice packets received on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.

On the constituent links, verify the following:

- The total number of packets transiting Q0 (350+350) matches the number of data packets and data fragments (500+200). If the numbers match, all the data packets after fragmentation correctly transited Q0 of the constituent links.

  Packets transited both constituent links, indicating that load balancing was correctly performed on non-LFI packets.

- The total number of packets transiting Q2 (300+100) on constituent links matches the number of voice packets received (400) on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.

  LFI packets from source port **100** transited **se-1/0/0**, and LFI packets from source port **200** transited **se-1/0/1**. Thus all LFI (Q2) packets were hashed based on the source port and correctly transited both constituent links.

Corrective Action—If the packets transited only one link, take the following steps to resolve the problem:

a. Determine whether the physical link is **up** (operational) or **down** (unavailable). An unavailable link indicates a problem with the PIM, interface port, or physical connection (link-layer errors). If the link is operational, move to the next step.

b. Verify that the classifiers are correctly defined for non-LFI packets. Make sure that non-LFI packets are not configured to be queued to Q2. All packets queued to Q2 are treated as LFI packets.

c. Verify that at least one of the following values is different in the LFI packets: source address, destination address, IP protocol, source port, or destination port. If the same values are configured for all LFI packets, the packets are all hashed to the same flow and transit the same link.

4. Use the results to verify load balancing.

Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device

Problem

Description: You are configuring a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces on a Juniper Networks device and a third-party device, and packets are being dropped and ping fails.

Solution

If the third-party device does not have the same FRF.12 support as the Juniper Networks device or supports FRF.12 in a different way, the Juniper Networks device interface on the PVC might discard a fragmented packet containing FRF.12 headers and count it as a "Policed Discard."

As a workaround, configure multilink bundles on both peers, and configure fragmentation thresholds on the multilink bundles.

Troubleshooting Security Policies

IN THIS SECTION

- Synchronizing Policies Between Routing Engine and Packet Forwarding Engine | 1700
- Checking a Security Policy Commit Failure | 1701
- Verifying a Security Policy Commit | 1701
- Debugging Policy Lookup | 1702

Synchronizing Policies Between Routing Engine and Packet Forwarding Engine

Problem

Description: Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.
- An error with the routing engine, such as a reused policy UID.

Environment: The policies in the Routing Engine and Packet Forwarding Engine must be in sync for the configuration to be committed. However, under certain circumstances, policies in the Routing Engine and the Packet Forwarding Engine might be out of sync, which causes the commit to fail.

Symptoms: When the policy configurations are modified and the policies are out of sync, the following error message displays - **error: Warning: policy might be out of sync between RE and PFE <*SPU-name(s)*> Please request security policies check/resync.**

Solution

Use the **show security policies checksum** command to display the security policy checksum value and use the **request security policies resync** command to synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine, if the security policies are out of sync.

SEE ALSO

show security policies checksum

> *request security policies check*
>
> *request security policies resync*

Checking a Security Policy Commit Failure

Problem

Description: Most policy configuration failures occur during a commit or runtime.

Commit failures are reported directly on the CLI when you execute the CLI command **commit-check** in configuration mode. These errors are configuration errors, and you cannot commit the configuration without fixing these errors.

Solution

To fix these errors, do the following:

1. Review your configuration data.
2. Open the file /var/log/nsd_chk_only. This file is overwritten each time you perform a commit check and contains detailed failure information.

Verifying a Security Policy Commit

Problem

Description: Upon performing a policy configuration commit, if you notice that the system behavior is incorrect, use the following steps to troubleshoot this problem:

Solution

1. Operational **show** Commands—Execute the operational commands for security policies and verify that the information shown in the output is consistent with what you expected. If not, the configuration needs to be changed appropriately.
2. Traceoptions—Set the **traceoptions** command in your policy configuration. The flags under this hierarchy can be selected as per user analysis of the **show** command output. If you cannot determine what flag to use, the flag option **all** can be used to capture all trace logs.

```
user@host# set security policies traceoptions <flag all>
```

You can also configure an optional filename to capture the logs.

```
user@host# set security policies traceoptions <filename>
```

If you specified a filename in the trace options, you can look in the /var/log/<*filename*> for the log file to ascertain if any errors were reported in the file. (If you did not specify a filename, the default filename is eventd.) The error messages indicate the place of failure and the appropriate reason.

After configuring the trace options, you must recommit the configuration change that caused the incorrect system behavior.

Debugging Policy Lookup

Problem
Description: When you have the correct configuration, but some traffic was incorrectly dropped or permitted, you can enable the **lookup** flag in the security policies traceoptions. The **lookup** flag logs the lookup related traces in the trace file.

Solution

```
user@host# set security policies traceoptions <flag lookup>
```

Log Error Messages used for Troubleshooting ISSU-Related Problems

IN THIS SECTION

- Chassisd Process Errors | **1702**
- Understanding Common Error Handling for ISSU | **1703**
- ISSU Support-Related Errors | **1706**
- Initial Validation Checks Failure | **1707**
- Installation-Related Errors | **1708**
- Redundancy Group Failover Errors | **1709**
- Kernel State Synchronization Errors | **1709**

The following problems might occur during an ISSU upgrade. You can identify the errors by using the details in the logs. For detailed information about specific system log messages, see System Log Explorer.

Chassisd Process Errors

Problem
Description: Errors related to chassisd.

Solution

Use the error messages to understand the issues related to chassisd.

When ISSU starts, a request is sent to chassisd to check whether there are any problems related to the ISSU from a chassis perspective. If there is a problem, a log message is created.

Understanding Common Error Handling for ISSU

Problem

Description: You might encounter some problems in the course of an ISSU. This section provides details on how to handle them.

Solution

Any errors encountered during an ISSU result in the creation of log messages, and ISSU continues to function without impact to traffic. If reverting to previous versions is required, the event is either logged or the ISSU is halted, so as not to create any mismatched versions on both nodes of the chassis cluster. Table 206 on page 1703 provides some of the common error conditions and the workarounds for them. The sample messages used in the Table 206 on page 1703 are from the SRX1500 device and are also applicable to all supported SRX Series devices.

Table 206: ISSU-Related Errors and Solutions

Error Conditions	Solutions
Attempt to initiate an ISSU when previous instance of an ISSU is already in progress	The following message is displayed: **warning: ISSU in progress** You can abort the current ISSU process, and initiate the ISSU again using the **request chassis cluster in-service-upgrade abort** command.

Table 206: ISSU-Related Errors and Solutions *(continued)*

Error Conditions	Solutions

Reboot failure on the secondary node	No service downtime occurs, because the primary node continues to provide required services. Detailed console messages are displayed requesting that you manually clear existing ISSU states and restore the chassis cluster.
	
	`error: [Oct  6 12:30:16]: Reboot secondary node failed (error-code: 4.1)`
	
	`error: [Oct  6 12:30:16]: ISSU Aborted! Backup node maybe in inconsistent state, Please restore backup node`
	`[Oct  6 12:30:16]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`
	
	Starting with Junos OS Release 17.4R1, the hold timer for the initial reboot of the secondary node during the ISSU process is extended from 15 minutes (900 seconds) to 45 minutes (2700 seconds) in chassis clusters on SRX1500, SRX4100, SRX4200, and SRX4600 devices.

Table 206: ISSU-Related Errors and Solutions *(continued)*

Error Conditions	Solutions

Secondary node failed to complete the cold synchronization	The primary node times out if the secondary node fails to complete the cold synchronization. Detailed console messages are displayed that you manually clear existing ISSU states and restore the chassis cluster. No service downtime occurs in this scenario.
	
	`[Oct  3 14:00:46]: timeout waiting for secondary node node1 to sync(error-code: 6.1)`
	`Chassis control process started, pid 36707`
	
	`error: [Oct  3 14:00:46]: ISSU Aborted! Backup node has been upgraded, Please restore backup node`
	`[Oct  3 14:00:46]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`

Table 206: ISSU-Related Errors and Solutions *(continued)*

Error Conditions	Solutions

Failover of newly upgraded secondary failed	No service downtime occurs, because the primary node continues to provide required services. Detailed console messages are displayed requesting that you manually clear existing ISSU states and restore the chassis cluster.
	
	`[Aug 27 15:28:17]: Secondary node0 ready for failover.`
	`[Aug 27 15:28:17]: Failing over all redundancy-groups to node0`
	`ISSU: Preparing for Switchover`
	`error: remote rg1 priority zero, abort failover.`
	`[Aug 27 15:28:17]: failover all RGs to node node0 failed (error-code: 7.1)`
	`error: [Aug 27 15:28:17]: ISSU Aborted!`
	`[Aug 27 15:28:17]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command`
	`otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`
	`{primary:node1}`

Upgrade failure on primary	No service downtime occurs, because the secondary node fails over as primary and continues to provide required services.
Reboot failure on primary node	Before the reboot of the primary node, devices being out of the ISSU setup, no ISSU-related error messages are displayed. The following reboot error message is displayed if any other failure is detected: `Reboot failure on Primary node` `Before the reboot of primary node, devices will be out of ISSU setup and no primary node error messages will be displayed.`

ISSU Support-Related Errors

Problem

Description: Installation failure occurs because of unsupported software and unsupported feature configuration.

Solution

Use the following error messages to understand the compatibility-related problems:

```
WARNING: Current configuration not compatible with
/var/tmp/junos-srx5000-11.4X3.2-domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
```

Initial Validation Checks Failure

Problem

Description: The initial validation checks fail.

Solution

The validation checks fail if the image is not present or if the image file is corrupt. The following error messages are displayed when initial validation checks fail when the image is not present and the ISSU is aborted:

When Image Is Not Present

```
user@host> ...0120914_srx_12q1_major2.2-539764-domestic.tgz reboot
Chassis ISSU Started
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade
Initiating in-service-upgrade
Fetching package...
error: File does not exist:
/var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-domestic.tgz
error: Couldn't retrieve package
/var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted
Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.
```

When Image File Is Corrupted

If the image file is corrupted, the following output displays:

```
user@host> ...junos-srx1k3k-11.4X9-domestic.tgz_1 reboot
Chassis ISSU Started
node1:
--------------------------------------------------------------------------
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade

node1:
--------------------------------------------------------------------------
Initiating in-service-upgrade
ERROR: Cannot use /var/tmp/junos-srx1k3k-11.4X9-domestic.tgz_1:
gzip: stdin: invalid compressed data--format violated
tar: Child returned status 1
tar: Error exit delayed from previous errors
ERROR: It may have been corrupted during download.
ERROR: Please try again, making sure to use a binary transfer.
Exiting in-service-upgrade window

node1:
--------------------------------------------------------------------------
Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted

node1:
--------------------------------------------------------------------------
Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.

{primary:node0}
```

The primary node validates the device configuration to ensure that it can be committed using the new software version. If anything goes wrong, the ISSU aborts and error messages are displayed.

Installation-Related Errors

Problem
Description: The install image file does not exist or the remote site is inaccessible.

Solution

Use the following error messages to understand the installation-related problems:

```
error: File does not exist: /var/tmp/junos-srx5000-11.4X3.2-domest
error: Couldn't retrieve package /var/tmp/junos-srx5000-11.4X3.2-domest
```

ISSU downloads the install image as specified in the ISSU command as an argument. The image file can be a local file or located at a remote site. If the file does not exist or the remote site is inaccessible, an error is reported.

Redundancy Group Failover Errors

Problem
Description: Problem with automatic redundancy group (RG) failure.

Solution
Use the following error messages to understand the problem:

```
failover all RG 1+ groups to node 0
error: Command failed.  None of the redundancy-groups has been failed over.
       Some redundancy-groups on node1 are already in manual failover mode.
       Please execute 'failover reset all' first..
```

Kernel State Synchronization Errors

Problem
Description: Errors related to ksyncd.

Solution
Use the following error messages to understand the issues related to ksyncd:

```
Failed to get kernel-replication error information from Standby Routing Engine.
```

```
mgd_slave_peer_has_errors() returns error at line 4414 in mgd_package_issu.
```

ISSU checks whether there are any ksyncd errors on the secondary node (node 1) and displays the error message if there are any problems and aborts the upgrade.

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, the hold timer for the initial reboot of the secondary node during the ISSU process is extended from 15 minutes (900 seconds) to 45 minutes (2700 seconds) in chassis clusters on SRX1500, SRX4100, SRX4200, and SRX4600 devices.

PART 13

Configuration Statements

Configuration Statements: Real-Time Performance Monitoring | **1713**

Configuration Statements: Ethernet OAM Connectivity Fault Management | **1752**

Configuration Statements: Ethernet OAM Link Fault Management | **1849**

Configuration Statements: sFlow Technology | **1928**

Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options | **1952**

Configuration Statements: Chassis Cluster | **1983**

Configuration Statements: Datapath Debug | **1994**

Configuration Statements: Health Monitoring | **2011**

Configuration Statements: Remote Monitoring (RMON) | **2021**

Configuration Statements: Resource Monitoring for Memory Regions | **2039**

Configuration Statements: Security Alarms | **2056**

Configuration Statements: Network Analytics | **2059**

Configuration Statements: SNMP | **2118**

Configuration Statements: SNMPv3 | **2282**

Configuration Statements: Uplink Failure Detection | **2342**

Cofiguration Statements: Port Mirroring and Analyzers | **2350**

Configuration Statements: TWAMP | **2428**

Configuration Statements: Tracing and System Logging | **2435**

Configuration Statement: App-Engine | **2528**

CHAPTER 59

Configuration Statements: Real-Time Performance Monitoring

IN THIS CHAPTER

- data-fill | **1714**
- data-size | **1715**
- destination-port | **1717**
- dscp-code-point | **1719**
- hardware-timestamp | **1721**
- history-size | **1722**
- moving-average-size | **1723**
- one-way-hardware-timestamp | **1724**
- port (RPM) | **1725**
- probe | **1726**
- probe-count | **1729**
- probe-interval | **1730**
- probe-limit | **1731**
- probe-server | **1732**
- probe-type | **1733**
- routing-instance | **1734**
- routing-instance (Syslog) | **1735**
- routing-instances | **1736**
- rpm (Interfaces) | **1737**
- rpm (Services) | **1738**
- source-address (Services) | **1742**
- tcp | **1743**
- test | **1744**
- test-interval | **1746**
- thresholds (Junos OS) | **1747**
- traps | **1749**
- udp | **1751**

data-fill

Syntax

```
data-fill data;
data-fill-with-zeros data;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 9.3 for PTX Series Packet Transport routers.
Statement at the [edit services rpm twamp client control-connection *control-client-name*] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes. The **data-fill** statement is not valid with the **http-get** or **http-metadata-get** probe types. For TWAMP client, if this knob is set, then fill the test packet with zeros, if the knob is not set then the data content is random value as indicated in RFC.

Options

data—A hexadecimal value; for example, **0-9**, **A-F**.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring BGP Neighbor Discovery Through RPM

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

data-size

Syntax

```
data-size size;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name test-session session-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the size of the data portion of ICMP probes. The **data-size** statement is not valid with the **http-get** or **http-metadata-get** probe type.

Options

size—0 through 65400 for RPM, for TWAMP the value is from 60 through 1400.

Default: 0 for RPM and 60 for TWAMP.

> **NOTE:** If you configure the hardware timestamp feature (see *Configuring RPM Timestamping on MX, M, T, and PTX Series Routers and EX Series Switches*):
>
> - The default value of **data-size** is 32 bytes and **32** is the minimum value for explicit configuration. The UDP timestamp probe type is an exception; it requires a minimum data size of 52 bytes.
> - The data size must be at least 100 bytes smaller than the default MTU of the interface of the RPM client interface.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Configuring BGP Neighbor Discovery Through RPM*

destination-port

Syntax

```
destination-port port;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Series Packet Transport Routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port to which a probe is sent. This statement is used only for TCP or UDP probe types.

The value for the **destination-port** can be only 7 when you configure the destination port along with hardware timestamping. A constraint check prevents you for configuring any other value for the destination port in this case.

This constraint does not apply when you are using one-way hardware timestamping along with **destination-port** and either **probe-type udp-ping** or **probe-type udp-ping-timestamp**.

Options

Default: The default value for the port is 862 to which the TWAMP client establishes control connection.

port—Port number **7** or from **49,160** through **65,535**.

> **NOTE:** The specified port numbers are recommended for RPM only.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring BGP Neighbor Discovery Through RPM

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

dscp-code-point

Syntax

```
dscp-code-point dscp-bits;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name test-session session-name]
```

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 for PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DiffServ code point (DSCP) bits value must be set to a valid 6-bit pattern.

Options

dscp-bits—A valid 6-bit pattern; for example, **001111**, or one of the following configured DSCP aliases:

- **af11**—Default: 001010
- **af12**—Default: 001100
- **af13**—Default: 001110
- **af21**—Default: 010010
- **af22**—Default: 010100
- **af23** —Default: 010110
- **af31** —Default: 011010
- **af32** —Default: 011100
- **af33** —Default: 011110
- **af41** —Default: 100010
- **af42** —Default:100100
- **af43** —Default:100110
- **be**—Default: 000000

- **cs1**—Default: 001000
- **cs2**—Default: 010000
- **cs3**—Default: 011000
- **cs4**—Default: 100000
- **cs5**—Default: 101000
- **cs6**—Default: 110000
- **cs7**—Default: 111000
- **ef**—Default: 101110
- **nc1**—Default: 110000
- **nc2**—Default: 111000

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

RELATED DOCUMENTATION

> *Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches*
>
> *Understanding Two-Way Active Measurement Protocol on Routers*

hardware-timestamp

Syntax

```
hardware-timestamp;
```

Hierarchy Level

[edit services rpm probe *owner* test *test-name*]

Release Information

Statement introduced in Junos OS Release 8.1.
Statement applied to MX Series routers in Junos OS Release 10.0.
Statement introduced in Junos OS Release 10.3 for EX Series switches.
Statement introduced in Junos OS Release 19.1 for PTX Series routers.
Statement introduced in Junos OS Release 19.2R1 for MPC10E-15C-MRATE on MX240, MX480, and MX960 routers.
Statement introduced in Junos OS Release 19.2R1 for MPC11E on MX2008, MX2010, and MX2020 routers.

Description

Enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor. This feature is supported only with **icmp-ping**, **icmp-ping-timestamp**, **udp-ping**, and **udp-ping-timestamp** probe types.

Required Privilege Level

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

history-size

Syntax

```
history-size size;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Series Packet Transport routers.
Statement at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the number of stored history entries.

Options

size—Value from 0 to 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

Configuring BGP Neighbor Discovery Through RPM

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

moving-average-size

Syntax

```
moving-average-size number;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement Introduced in Junos OS Release 13.2 for PTX Series Packet Transport routers.
Statement at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Enable statistical calculation operations to be performed across a configurable number of the most recent samples.

Options

number—Number of samples to be used in calculations.

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 RPM Probes on M, MX and T Series Routers and EX Series Switches

one-way-hardware-timestamp

Syntax

```
one-way-hardware-timestamp;
```

Hierarchy Level

[edit services rpm **probe** *owner* **test** *test-name*]

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 19.1 for PTX Series routers.
Statement introduced in Junos OS Release 19.2R1 for MPC10E-15C-MRATE on MX240, MX480, and MX960 routers.
Statement introduced in Junos OS Release 19.2R1 for MPC11E on MX2008, MX2010, and MX2020 routers.

Description

Enable timestamping of RPM probe messages for one-way delay and jitter measurements. You must configure this statement along with the **destination-interface** statement to invoke timestamping. This feature is supported only with **icmp-ping**, **icmp-ping-timestamp**, **udp-ping**, and **udp-ping-timestamp** probe types.

NOTE: Starting in Junos OS Evolved Release 20.1R1, the function provided by this command has been replaced by the **offload-type (none|pfe-timestamp)** command.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring RPM Timestamping on MX, M, T, and PTX Series Routers and EX Series Switches

destination-interface

hardware-timestamp | **1721**

port (RPM)

Syntax

```
port number;
```

Hierarchy Level

```
[edit services rpm probe-server (tcp | udp)]
```

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 PTX Series Packet Transport routers.

Description

Specify the port number for the probe server.

Options

number—Port number for the probe server. The value can be **7** or **49,160** 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 RPM Receiver Servers

probe

Syntax

```
probe owner {
    test test-name {
        data-fill data;
        data-size size;
        delegate-probes probes;
        destination-interface interface-name;
        destination-port port;
        dscp-code-point dscp-bits;
        history-size size;
        inet6-options source-address ipv6-address;
        moving-average-size number;
        next-hop next-hop;
        offload-type {
            none;
            pfe-timestamp;
        }
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instance instance-name;
        rpm-scale {
            destination {
                interface interface-name.logical-unit-number;
                subunit-cnt subunit-cnt;
            }
            source {
                address-base ipv4-address-base;
                count ipv4-count;
                step ipv4-step;
            }
            source-inet6 {
                address-base ipv6-address-base;
                count ipv6-count;
                step ipv6-step;
            }
            target {
                address-base ipv4-address-base;
                count ipv4-count;
                step ipv4-step;
            }
            target-inet6 {
```

```
            address-base ipv6-address-base;
            count ipv6-count;
            step ipv6-step;
          }
          tests-count tests-count;
        }
        source-address address;
        target (url url | address ipv4-address | inet6-url url | inet6-address ipv6-address);
        test-interval interval;
        thresholds
        {
          egress-time microseconds;
          ingress-time microseconds;
          jitter-egress microseconds;
          jitter-ingress microseconds;
          jitter-rtt microseconds;
          rtt microseconds;
          std-dev-egress microseconds;
          std-dev-ingress microseconds;
          std-dev-rtt microseconds;
          successive-loss count;
          total-loss count;
        }
        traps [trap-names];
        ttl [hop-count];
    }
}
```

Hierarchy Level

```
[edit services rpm]
```

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 18.1 for QFX Series switches.

Description

Specify an owner name. The owner name combined with the test name represent a single RPM configuration instance.

Options

owner—Owner name up to 32 characters in length.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

probe-count

Syntax

```
probe-count count;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name test-session session-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the number of probes within a test.

Options

count—1 through 15 for RPM, for TWAMP 1 through 4,294,967,290.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring BGP Neighbor Discovery Through RPM

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

probe-interval

Syntax

```
probe-interval interval;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name test-session session-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Specify the time to wait between sending packets, in seconds.

Options

interval—Number of seconds, from 1 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 BGP Neighbor Discovery Through RPM*
- *Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches*
- *Understanding Two-Way Active Measurement Protocol on Routers*

probe-limit

Syntax

```
probe-limit limit;
```

Hierarchy Level

```
[edit services rpm]
```

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 PTX Series Packet Transport routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Configure the maximum number of concurrent probes allowed.

Options

limit—Maximum number of concurrent probes allowed.

Range: (MX Series routers only) Starting in Junos OS Release 17.2R2 and 17.3R1, 1 through 2000. In Junos releases earlier than 17.2R1, the range is 1 through 500.

Range: (PTX Series Packet Transport routers only) 1 through 200

Range: (Other platforms) 1 through 500

Default: 100

Required Privilege Level

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

RELATED DOCUMENTATION

Limiting the Number of Concurrent RPM Probes on M, MX, T and PTX Routers and EX Series Switches

probe-server

Syntax

```
probe-server {
    tcp {
        destination-interface interface-name;
        port number;
    }
    udp {
        destination-interface interface-name;
        port number;
    }
}
```

Hierarchy Level

```
[edit services rpm]
```

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 PTX Series Packet Transport routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Specify the server to act as a receiver for the probes.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The **destination-interface** statement is not supported on PTX Series routers.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring RPM Receiver Servers

probe-type

Syntax

```
probe-type type;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name]
```

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 PTX Series Packet Transport routers.

Description

Specify the packet and protocol contents of a probe.

Options

type—One of the following probe type values:

- **http-get**—(Not available at the **[edit services rpm bgp]** hierarchy level.) Sends a Hypertext Transfer Protocol (HTTP) get request to a target URL.
- **http-metadata-get**—(Not available at the **[edit services rpm bgp]** hierarchy level.) Sends an HTTP get request for metadata to a target URL.
- **icmp-ping**—Sends ICMP echo requests to a target address.
- **icmp-ping-timestamp**—Sends ICMP timestamp requests to a target address.
- **tcp-ping**—Sends TCP packets to a target.
- **udp-ping**—Sends UDP packets to a target.
- **udp-ping-timestamp**—Sends UDP timestamp requests to a target address.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring BGP Neighbor Discovery Through RPM

routing-instance

Syntax

```
routing-instance instance-name;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name]
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the routing instance used by the probes. The routing instance is also applicable for control connection.

> **NOTE:** The media interface from where the TWAMP control and test or data packets arrive and exit the **si- logical interface** must be a part of the same routing instance.

Options

instance-name—Routing instance configured at the **[edit routing-instance]** hierarchy level.

Default: Internet (IPv4) 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

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

Understanding Two-Way Active Measurement Protocol on Routers

routing-instance (Syslog)

Syntax

```
routing-instance routing-instance-name;
```

Hierarchy Level

```
[edit system syslog],
[edit system syslog host ip-address]
```

Release Information

Statement introduced in Junos OS Release 18.4R1.

Description

Configure the routing instance name for the routing instance that you want the syslog client to use. If you want to use the reserved non-default management routing instance mgmt_junos, make sure you configure the **management-instance** statement.

> **NOTE:** You must also define the routing instance you want to use under the **[edit routing-instances]** hierarchy level.

Starting in Junos OS Evolved Release 20.1R1 and 19.4R2, if you are sending syslog messages to a remote host that is identified by its IP address at the **[edit system syslog host *ip-address*]** hierarchy, you only need to configure the **management-instance** statement to use the mgmt_junos routing instance. You do not need to configure the mgmt_junos routing instance at the **[edit system syslog host *ip-address* routing-instance]** hierarchy.

Required Privilege Level

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

RELATED DOCUMENTATION

Management Interface in a Non-Default Instance

routing-instances

Syntax

```
routing-instances instance-name;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm bgp logical-system logical-system-name]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport routers.

Description

Specify the routing instance used by the probes.

Options

instance-name—A routing instance configured at the **[edit routing-instances]** hierarchy level.

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

Configuring BGP Neighbor Discovery Through RPM

rpm (Interfaces)

Syntax

```
rpm (client client | server server | twamp-client twamp-client | twamp-server twamp-server);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description

Associate an RPM or TWAMP client (router or switch that originates RPM or TWAMP probes) or RPM or TWAMP server with a specified interface.

NOTE: The TWAMP client is applicable only for **si-** interfaces.

Options

client—Identifier for RPM client router or switch.

server—Identifier for RPM server.

twamp-client—Identifier for RPM TWAMP client router.

twamp-server—Identifier for RPM TWAMP server.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring RPM Timestamping on MX, M, T, and PTX Series Routers and EX Series Switches

rpm (Services)

Syntax

```
rpm {
    bgp {
        data-fill data;
        data-size size;
        destination-port port;
        history-size size;
        logical-system logical-system-name [routing-instances routing-instance-name];
        moving-average-size number;
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instances instance-name;
        test-interval interval;
    }
    probe owner {
        test test-name {
            data-fill data;
            data-size size;
            destination-interface interface-name;
            destination-port port;
            dscp-code-point dscp-bits;
            hardware-timestamp;
            history-size size;
            moving-average-size number;
            one-way-hardware-timestamp;
            probe-count count;
            probe-interval seconds;
            probe-type type;
            routing-instance instance-name;
            source-address address;
            target (url url | address address);
            test-interval interval;
            thresholds thresholds;
            traps traps;
        }
    }
    probe-server {
        tcp {
            destination-interface interface-name;
            port number;
        }
```

```
    udp {
        destination-interface interface-name;
        port number;
    }
}
probe-limit limit;
rfc2544-benchmarking {
    profiles {
        test-profile profile-name {
            test-type (throughput | latency | frame-loss | back-back-frames);
            packet-size bytes;
            step-percent percent;
            bandwidth-kbps kpbs;
        }
    }
    tests{
        test-name test-name {
            test-interface interface-name;
            mode reflect;
            family (bridge| inet | ccc);
            destination-ipv4-address address;
            destination-udp-port port-number;
            source-ipv4-address address;
            source-udp-port port-number;
            direction (egress | ingress);
        }
    }
}
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag;
}
```

```
    twamp {
        server {
            authentication-mode (authenticated | encrypted | none);
            authentication-key-chain identifier {
                key-id identifier {
                    secret password-string;
                }
            }
            client-list list-name {
                [ address address ];
            }
            inactivity-timeout seconds;
            maximum-connections-duration hours;
            maximum-connections count;
            maximum-connections-per-client count;
            maximum-sessions count;
            maximum-sessions-per-connection count;
            port number;
            routing-instance-list {
                instance-name {
                    port number;
                }
            }
            server-inactivity-timeout minutes;
            tcp-keepcnt
            tcp-keepidle
            tcp-keepintvl
        }
    }
    rfc2544-benchmarking {
        tests{
            test-name test-name {
                test-interface interface-name;
                mode reflect;
                family (inet | ccc);
                destination-ipv4-address address;
                destination-udp-port port-number;
                source-ipv4-address address;
                source-udp-port port-number;
                direction (egress | ingress);
            }
        }
    }
}
```

Hierarchy Level

[edit services]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure BGP neighbor discovery through RPM.

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 BGP Neighbor Discovery Through RPM*

source-address (Services)

Syntax

```
source-address address;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name]
```

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 PTX Series Packet Transport routers.

Description

Specify the source IP address used for probes. If the source IP address is not one of the router's or switch's assigned addresses, the packet use the outgoing interface's address as its source.

The following addresses cannot be used for the source IP address used for probes:

- 0.0.0.0
- 127.0.0.0/8 (loopback)
- 224.0.0.0/4 (multicast)
- 255.255.255.255 (broadcast)

Options

address—Valid IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

tcp

Syntax

```
tcp {
    destination-interface interface-name;
    port port;
}
```

Hierarchy Level

```
[edit services rpm probe-server]
```

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 PTX Series Packet Transport routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Specify the port information for the TCP server.

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 RPM Receiver Servers

test

Syntax

```
test test-name {
    data-fill data;
    data-size size;
    destination-interface interface-name;
    destination-port port;
    dscp-code-point dscp-bits;
    hardware-timestamp;
    history-size size;
    moving-average-size number;
    inet6-options;
    one-way-hardware-timestamp;
    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance instance-name;
    rpm-scale {
        destination {
            interface interface-name.logical-unit-number;
            subunit-cnt subunit-cnt;
        }
        source {
            address-base ipv4-address-base;
            count ipv4-count;
            step ipv4-step;
        }
        source-inet6 {
            address-base ipv6-address-base;
            count ipv6-count;
            step ipv6-step;
        }
        target {
            address-base ipv4-address-base;
            count ipv4-count;
            step ipv4-step;
        }
        target-inet6 {
            address-base ipv6-address-base;
            count ipv6-count;
            step ipv6-step;
        }
        tests-count tests-count;
```

```
    }
    source-address address;
    target (url url | address address);
    test-interval interval;
    thresholds thresholds;
    traps traps;
    ttl hop-count
}
```

Hierarchy Level

```
[edit services rpm probe owner]
```

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 PTX Series Packet Transport routers.
inet6-options option added in Junos OS Release 14.1R4 for MX Series routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Specify the range of probes over which the standard deviation, average, and jitter are calculated. The test name combined with the owner name represent a single RPM configuration instance.

Options

test-name—Test name. The name can be up to 32 characters in length.

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 RPM Probes on M, MX and T Series Routers and EX Series Switches

test-interval

Syntax

```
test-interval seconds;
```

Hierarchy Level

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify the time to wait between tests, in seconds. A test interval of 0 seconds causes the RPM test to stop after one iteration.

Options

seconds—Number of seconds to wait between tests.

Range: **[edit services rpm bgp]** and **[edit services rpm probe *owner* test *test-name*]** hierarchy levels: 0 through 86,400

Range: **[edit services rpm twamp client control-connection *control-client-name*]** hierarchy level: 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 BGP Neighbor Discovery Through RPM*
- *Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches*
- *Understanding Two-Way Active Measurement Protocol on Routers*

thresholds (Junos OS)

Syntax

```
thresholds thresholds;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Packet Series Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Specify thresholds used for the probes. A system log message is generated when the configured threshold is exceeded. Likewise, an SNMP trap (if configured) is generated when a threshold is exceeded.

> **NOTE:** If you configure a value of zero using the ***thresholds*** option for a certain probe parameter, the generation of SNMP traps is disabled for the corresponding probe attribute. For example, if you specify the **set thresholds jitter-egress 0** statement, it denotes that traps are not triggered when the jitter in egress time threshold is met or exceeded.

Options

thresholds—Specify one or more threshold measurements. The following options are supported:

- **egress-time**—Measures maximum source-to-destination time per probe.
- **ingress-time**—Measures maximum destination-to-source time per probe.
- **jitter-egress**—Measures maximum source-to-destination jitter per test.
- **jitter-ingress**—Measures maximum destination-to- source jitter per test.
- **jitter-rtt**—Measures maximum jitter per test, from 0 through 60,000,000 microseconds.
- **rtt**—Measures maximum round-trip time per probe, in microseconds.
- **std-dev-egress**—Measures maximum source-to-destination standard deviation per test.

- **std-dev-ingress**—Measures maximum destination-to-source standard deviation per test.
- **std-dev-rtt**—Measures maximum standard deviation per test, in microseconds.
- **successive-loss**—Measures successive probe loss count, indicating probe failure.
- **total-loss**—Measures total probe loss count indicating test failure, from 0 through 15.

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

RELATED DOCUMENTATION

> *Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches*
>
> *Understanding Two-Way Active Measurement Protocol on Routers*

traps

Syntax

```
traps traps;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name],
[edit services rpm twamp client control-connection control-client-name]
```

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 PTX Series Packet Transport routers.
Support at the [**edit services rpm twamp client control-connection *control-client-name***] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.

Description

Set the trap bit to generate traps for probes. Traps are sent if the configured threshold is met or exceeded.

Options

traps—Specify one or more traps. The following options are supported:

- **control-connection-closed**—Generate traps when the control connection is closed.
- **egress-jitter-exceeded**—Generate traps when the jitter in egress time threshold is met or exceeded.
- **egress-std-dev-exceeded**—Generate traps when the egress time standard deviation threshold is met or exceeded.
- **egress-time-exceeded**—Generate traps when the maximum egress time threshold is met or exceeded.
- **ingress-jitter-exceeded**—Generate traps when the jitter in ingress time threshold is met or exceeded.
- **ingress-std-dev-exceeded**—Generate traps when the ingress time standard deviation threshold is met or exceeded.
- **ingress-time-exceeded**—Generate traps when the maximum ingress time threshold is met or exceeded.
- **jitter-exceeded**—Generate traps when the jitter in round-trip time threshold is met or exceeded.
- **probe-failure**—Generate traps when successive probe loss thresholds are crossed.
- **rtt-exceeded**—Generate traps when the maximum round-trip time threshold is met or exceeded.
- **std-dev-exceeded**—Generate traps when the round-trip time standard deviation threshold is met or exceeded.

- **test-completion**—Generate traps when a test is completed.
- **test-failure**—Generate traps when the total probe loss threshold is met or exceeded.
- **test-iteration-done**—Generate traps when all test sessions under control connections complete one test iteration.

> **NOTE:** For RPM traps to be generated, you must configure the **remote-operations** SNMP trap category by including the **categories** statement at the **[edit snmp trap-group *trap-group-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

Configuring RPM Probes on M, MX and T Series Routers and EX Series Switches

Understanding Two-Way Active Measurement Protocol on Routers

udp

Syntax

```
udp {
    destination-interface interface-name;
    port port;
}
```

Hierarchy Level

```
[edit services rpm probe-server]
```

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 PTX Series Packet Transport routers.
Statement introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Specify the port information for the UDP server.

The remaining statements are explained separately. See CLI Explorer.

> **NOTE:** The **destination-interface** statement is not supported on PTX Series routers.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring RPM Receiver Servers

CHAPTER 60

Configuration Statements: Ethernet OAM Connectivity Fault Management

IN THIS CHAPTER

- 802.3ad | **1755**
- action-profile (Applying to CFM) | **1756**
- action-profile (Defining for CFM) | **1757**
- action-profile (MEP) | **1759**
- adjacency-loss | **1760**
- ais-trigger-condition | **1761**
- all-defects | **1762**
- auto-discovery | **1763**
- avg-fd-twoway-threshold | **1764**
- avg-ifdv-twoway-threshold | **1766**
- avg-flr-forward-threshold | **1768**
- avg-flr-backward-threshold | **1770**
- calculation-weight | **1772**
- clear-action (CFM) | **1773**
- clear oam ethernet connectivity-fault-management event | **1774**
- connection-protection-tlv | **1776**
- continuity-check | **1777**
- convey-loss-threshold | **1778**
- cross-connect-ccm | **1779**
- cycle-time | **1780**
- data-tlv-size | **1781**
- default-actions | **1782**
- delay | **1783**
- delegate-server-processing | **1784**
- delay-variation | **1785**
- detect-loc | **1786**
- direction | **1788**

- enhanced-cfm-mode | **1789**
- erroneous-ccm | **1790**
- evc-protocol cfm | **1791**
- event (CFM) | **1793**
- flap-trap-monitor | **1794**
- hardware-assisted-timestamping | **1796**
- hardware-assisted-keepalives | **1797**
- hold-interval (OAM) | **1799**
- instance | **1800**
- interface (IEEE 802.1ag OAM Connectivity-Fault Management) | **1801**
- interface (OAM Link-Fault Management) | **1802**
- interface-down | **1803**
- interface-status-tlv | **1804**
- interface-status-send-rdi | **1805**
- interval | **1806**
- interval (CFM MEP) | **1808**
- iteration-count | **1809**
- iteration-period | **1810**
- level | **1811**
- level (CFM MEP) | **1812**
- linktrace | **1813**
- log-and-generate-ais | **1814**
- loss-threshold | **1815**
- lowest-priority-defect | **1816**
- maintenance-association | **1817**
- maintenance-domain | **1819**
- measurement-interval | **1821**
- measurement-type | **1822**
- mep | **1823**
- mip-half-function | **1825**
- name-format | **1826**
- no-aggregate-delegate-processing | **1827**
- path-database-size | **1828**
- performance-monitoring | **1829**

- policer (CFM Global) | **1831**
- policer (CFM Session) | **1832**
- port-status-tlv | **1833**
- priority (Protocols OAM) | **1834**
- priority (CFM MEP) | **1835**
- priority (OAM Connectivity-Fault Management) | **1836**
- protocol (Server MEP) | **1837**
- protect-maintenance-association (OAM) | **1838**
- rdi | **1839**
- receive-ais | **1840**
- remote-maintenance-association (OAM) | **1841**
- remote-mep | **1842**
- sendid-tlv | **1843**
- short-name-format | **1844**
- sla-iterator-profile | **1845**
- sla-iterator-profiles | **1847**

802.3ad

Syntax

```
802.3ad {
    primary | backup;
    ae interface-number ;
    lacp {
        port-priority priority-number;
    }
    link-index index-number
    distribution-list distribution-list-number
}
```

Hierarchy Level

```
[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.

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

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 | 40

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);
            levelvalue;
            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 | **65**
- default-actions | **1782**
- event (CFM) | **1793**
- interface-down | **1803**

action-profile (MEP)

Syntax

```
action-profile action-profile-name;
```

Hierarchy Level

```
[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 14.2.

Description

Attach the configured action profile to the MEP depending on the hierarchy level.

Options

action-profile-name—Name of the action profile that is configured for the CFM MEP and the server MEP.

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 | **286**

Configuring ETH-AIS on a CFM MEP | **292**

adjacency-loss

Syntax

```
adjacency-loss;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the defect condition that raises an alarm indication signal when physical connectivity is lost between peer MEPs.

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 | 286

Configuring ETH-AIS on a CFM MEP | 292

ais-trigger-condition

Syntax

```
ais-trigger-condition {
    adjacency-loss;
    all-defects;
    cross-connect-ccm;
    erroneous-ccm;
    receive-ais;
}
```

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management action-profile *action-profile-name* event]

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the defect conditions that generate an alarm indication signal (AIS).

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

Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286

Configuring ETH-AIS on a CFM MEP | 292

all-defects

Syntax

```
all-defects;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the defect condition that raises an alarm indication signal when any or all possible defects occur in the maintenance domain level.

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 | 286
Configuring ETH-AIS on a CFM MEP | 292

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 | 40

avg-fd-twoway-threshold

Syntax

```
avg-fd-twoway-threshold avg-fd-twoway-threshold-value{
flap-trap-monitor seconds;}
```

Hierarchy Level

[edit protocols oam **ethernet** connectivity-fault-management **performance-monitoring sla-iterator-profiles** *profile-name*]

Release Information

Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description

Configure the threshold value for average frame delay, in microseconds, for two-way Ethernet frame delay measurement (ETH-DM). When the configured threshold for average frame delay is exceeded, an SNMP trap is generated for ETH-DM. SNMP traps are triggered if you configure either the average frame-delay threshold or the average inter-frame delay variance threshold. If you do not configure either the frame-delay threshold or the frame delay variation threshold, no SNMP traps are generated. You can configure these threshold values only with a two-way ETH-DM SLA iterator.

Frame delay refers to the difference, in microseconds, between the time a frame is sent and when it is received. Frame delay variation refers to the difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.” For one-way Ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics.

Options

avg-fd-twoway-threshold-value—Threshold value for average frame delay, in microseconds, for two-way ETH-DM.

Range: 1 through 4294967295 microseconds

flap-trap-monitor *seconds*—Duration in seconds, for summarizing flap occurrences and send out a single jnxSoamPm ThresholdFlapAlarm notification to the network management system (NMS).

Range: 1 through 360 seconds

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

flap-trap-monitor | 1794

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

avg-ifdv-twoway-threshold

Syntax

```
avg-ifdv-twoway-threshold avg-ifdv-twoway-threshold-value; {
flap-trap-monitor seconds; }
```

Hierarchy Level

[edit protocols oam **ethernet** connectivity-fault-management **performance-monitoring sla-iterator-profiles** *profile-name*]

Release Information

Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description

Configure the threshold value for average frame delay variation, in microseconds, for two-way Ethernet frame delay measurement (ETH-DM). When the configured threshold for average frame delay variation is exceeded, an SNMP trap is generated for ETH-DM. SNMP traps are triggered if you configure either the average frame-delay threshold or the average inter-frame delay variance threshold. If you do not configure either the frame-delay threshold or the frame delay variation threshold, no SNMP traps are generated. You can configure these threshold values only with a two-way ETH-DM SLA iterator.

Frame delay refers to the difference, in microseconds, between the time a frame is sent and when it is received. Frame delay variation refers to the difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.” For one-way Ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics. In two-way ETH-DM mode, frame delay and frame delay variation values are based on the time difference between when the initiator MEP transmits a request frame and receives a reply frame from the responder MEP, subtracting the time elapsed at the responder MEP.

Options

avg-ifdv-twoway-threshold-value—Threshold value for average frame delay variation, in microseconds, for two-way ETH-DM.

Range: 1 through 4294967295 microseconds

flap-trap-monitor *seconds*—Duration in seconds, for summarizing flap occurrences and send out a single jnxSoamPm ThresholdFlapAlarm notification to the network management system (NMS).

Range: 1 through 360 seconds

Required Privilege Level

configure—To enter configuration mode.

control—To modify any configuration.

RELATED DOCUMENTATION

flap-trap-monitor | 1794

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

avg-flr-forward-threshold

Syntax

```
avg-flr-forward-threshold avg-flr-forward-threshold-value;{
flap-trap-monitor seconds; }
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description

Configure the threshold value for average frame loss ratio, in milli-percent, in the upstream or forward direction for Ethernet loss measurement (ETH-LM) and Ethernet synthetic loss measurement (ETH-SLM). When the configured threshold for average forward frame loss ratio is exceeded, an SNMP trap is generated for ETH-LM and ETH-SLM. SNMP traps are triggered if you configure either the average backward frame loss ratio threshold or the average forward frame loss ratio threshold. If you do not configure either the average backward frame loss ratio threshold or the average forward frame loss ratio threshold, no SNMP traps are generated. You can configure these threshold values with an SLA iterator for ETH-SLM and ETH-LM.

ETH-SLM is an application that enables the calculation of frame loss by using synthetic frames instead of data traffic. This mechanism can be considered as a statistical sample to approximate the frame loss ratio of data traffic.

Options

avg-flr-forward-threshold-value—Threshold value for average frame loss ratio in the forward or upstream direction, in milli-percent, for ETH-SLM and ETH-LM.

Range: 1 through 100000 milli-percent

flap-trap-monitor *seconds*—Duration in seconds, for summarizing flap occurrences and send out a single jnxSoamPm ThresholdFlapAlarm notification to the network management system (NMS).

Range: 1 through 360 seconds

Required Privilege Level

configure—To enter configuration mode.
control—To modify any configuration.

RELATED DOCUMENTATION

flap-trap-monitor | 1794

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

avg-flr-backward-threshold

Syntax

```
avg-flr-backward-threshold avg-flr-backward-threshold-value;{
flap-trap-monitor seconds; }
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description

Configure the threshold value for average frame loss ratio, in milli-percent, in the backward or downstream direction for Ethernet loss measurement (ETH-LM) and Ethernet synthetic loss measurement (ETH-SLM). When the configured threshold for average backward frame loss ratio is exceeded, an SNMP trap is generated for ETH-LM and ETH-SLM. SNMP traps are triggered if you configure either the average backward frame loss ratio threshold or the average forward frame loss ratio threshold. If you do not configure either the average backward frame loss ratio threshold or the average forward frame loss ratio threshold, no SNMP traps are generated. You can configure these threshold values with an SLA iterator for ETH-SLM and ETH-LM.

ETH-SLM is an application that enables the calculation of frame loss by using synthetic frames instead of data traffic. This mechanism can be considered as a statistical sample to approximate the frame loss ratio of data traffic.

Options

avg-flr-backward-threshold-value—Threshold value for average frame loss ratio in the backward or downstream direction, in milli-percent, for ETH-SLM and ETH-LM.

Range: 1 through 100000 milli-percent

flap-trap-monitor *seconds*—Duration in seconds, for summarizing flap occurrences and send out a single jnxSoamPm ThresholdFlapAlarm notification to the network management system (NMS).

Range: 1 through 360 seconds

Required Privilege Level

configure—To enter configuration mode.
control—To modify any configuration.

RELATED DOCUMENTATION

flap-trap-monitor | 1794

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

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 | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- delay | 1783
- delay-variation | 1785

clear-action (CFM)

Syntax

```
clear-action {
    interface-down peer-interface;
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name ]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Clear the action or actions to be taken when the connectivity fault management event occurs. You cannot configure multiple actions at this time. Only one action can be configured. This limitation affects both the **action** and **clear-action** statements.

Options

peer-interface—Name of the peer 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 CFM Action Profile to Specify CFM Actions for CFM Events | **65**

clear oam ethernet connectivity-fault-management event

Syntax

```
clear oam ethernet connectivity-fault-management event
(adjacency-loss| all-defects | cross-connect-ccm | erroneous-ccm | receive-ais)
maintenance-domain md-name
maintenance-association ma-name
local-mep local-mep-id
logical-system
remote-mep remote-mep-id
```

Release Information

Command introduced in Junos OS Release 20.2.

Description

Clear the event for the configured action profile. If you have configured the action profile at the local MEP level, when you clear the event for the configured action profile, you can specify only the local MEP numeric identifier to clear the event. You need not specify the remote MEP numeric identifier. If you have configured the action profile at the remote MEP level, when you clear the event for the configured action profile, you must specify both the local MEP numeric identifier and remote MEP numeric identifier to clear the event.

Options

adjacency loss—Clear the adjacency loss event.

all-defects—Clear the all-defects event.

cross-connect-ccm—Clear the cross-connect-ccm event.

erroneous-ccm—Clear the erroneous-ccm event.

local-mep *local-mep-id*—Specify the local MEP numeric identifier. If you have configured the action profile at the local MEP, you can clear the event for the configured action profile at the local MEP level. You need not specify the remote MEP numeric identifier.

logical-system—Name of the logical system

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

receive-ais—Clear the receive-ais event.

remote-mep *remote-mep-id*—Specify the remote MEP numeric identifier. If you have configured the action profile at the remote MEP, you can clear the event for the configured action profile at the remote

MEP level. You must specify both the local MEP numeric identifier and the remote MEP numeric identifier.

Required Privilege Level
view

List of Sample Output
clear oam ethernet connectivity-fault-management event on page 1775

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management event

`user@host>` **clear oam ethernet connectivity-fault-management event maintenance-domain md5 maintenance-association ma5 local-mep 2 remote-mep 1**

```
Action Profile Event Cleared.
```

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

Configuring MAC Flush Message Processing in CET Mode | 118

Example: Configuring an Action Profile Based on Connection Protection TLVs | 121

continuity-check

Syntax

```
continuity-check {
    convey-loss-threshold;
    hold-interval minutes;
    interface-status-tlv;
    interval (10m | 10s | 1m | 1s| 100ms | 10ms| 3.3ms);
    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.

> **NOTE:** When the continuity-check interval is set to 3.3ms, the actual interval is 4ms (250 pps).

Options

convey-loss-threshold—Enable loss-threshold-tlv transmission.

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 | 3.3ms)*—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 | 39

convey-loss-threshold

Syntax

```
convey-loss-threshold;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
   maintenance-association ma-name continuity-check]
```

Description

Enable loss-threshold-tlv transmission.

During a unified ISSU, the control plane may go down for several seconds and cause CFM continuity check packets to get dropped. This may cause the remote maintenance endpoint (MEP) to detect a connectivity loss and mark the MEP as down. To keep the MEP active during a unified ISSU, the loss threshold TLV communicates the minimum threshold value the receiving MEP requires to keep the MEP active. The receiving MEP parses the TLV and updates the loss threshold value, but only if the new threshold value is greater than the locally configured threshold value. You can control the transmission of the loss threshold TLV in continuity check messages PDUs. The **convey-loss-threshold** statement specifies that the loss threshold TLV must be transmitted as part of the continuity check messages. If the statement is not specified, continuity check messages transmit this TLV only when a unified ISSU is in progress.

Required Privilege Level

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

cross-connect-ccm

Syntax

```
cross-connect-ccm;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the defect condition that raises an alarm indication signal when any cross-connect continuity check messages (CCMs) are received by the MEP.

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 | 286
Configuring ETH-AIS on a CFM MEP | 292

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 Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

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 | 1845

Configuring a Remote MEP with an Iterator Profile | 270

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 | 65

delay

Syntax

```
delay delay-value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name calculation-weight]
```

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.

Options

delay-value—Calculation weight for delay.

> **NOTE:** This option is applicable only for two-way delay measurement.

Range: 1 through 65,535

Default: 1

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

- Configuring an Iterator Profile | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- calculation-weight | 1772

delegate-server-processing

Syntax

```
delegate-server-processing;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
```

Release Information
Statement introduced in Junos OS Release 11.1.

Description
For Ethernet interfaces on MX Series routers , enable server-side processing for two-way delay measurement and loss measurement.

By default, the processing is done by the Routing Engine.

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

RELATED DOCUMENTATION

Ethernet Frame Delay Measurements Overview | 166

delay-variation

Syntax

```
delay-variation delay-variation-value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name calculation-weight]
```

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 variation.

Options

delay-variation-value—Calculation weight for delay variation.

> **NOTE:** This option is applicable only for two-way delay measurement.

Range: 1 through 65,535

Default: 1

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

- Configuring an Iterator Profile | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- calculation-weight | 1772

detect-loc

Syntax

```
detect-loc;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association
    ma-name mep mep-id remote-mep mep-id ]
```

```
[edit protocols oam ethernet link-fault-management interface interface-name ]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Specify whether Ethernet OAM continuity checks are performed for an individual remote maintenance end point (MEP).

When you configure the **detect-loc** statement at [**edit protocols oam ethernet link-fault-management interface *interface-name***] hierarchy level, a loss-of-continuity (LOC) defect is raised when the peer is not found within a period that is equal to 3 times the current keepalive pdu interval. When an LOC defect is raised, a syslog error message is generated .

> **NOTE:** When you configure the **detect-loc** statement at the [**edit protocols oam ethernet link-fault-management interface *interface-name***] hierarchy level, any **action-profile** configured to bring down the interface is executed when an LOC defect is detected. However, the **action-profile** is not executed if you have not configured **detect-loc** statement the **detect-loc** statement at the [**edit protocols oam ethernet link-fault-management interface *interface-name***] hierarchy level.

To view the current LOC status of an interface, execute the **show oam ethernet link-fault-management** command.

Default

The MEP does not generate LOC defect messages by default.

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 | 40
- remote-mep | 1842

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 | 40

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

enhanced-cfm-mode

Syntax

```
enhanced-cfm-mode enhanced-cfm-mode;
```

Hierarchy Level

```
[edit logical-systems name protocols oam ethernet connectivity-fault-management],
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 17.2R1 for MX Series routers.

Description

Enables enhanced CFM mode. When you enable enhanced CFM mode, Junos OS supports 32, 000 maintenance association end points (MEPs) and maintenance intermediate points (MIPs) each per chassis for bridge, VPLS, L2VPN, and CCC domains. To support enhanced CFM mode, configure the network services mode on the router as **enhanced-ip**.

NOTE: After enabling CFM mode, restart CFM for the changes to take effect. If you do not restart CFM, CFM automatically restarts after 1 minute.

Required Privilege Level

Routing

RELATED DOCUMENTATION

Enabling Enhanced Connectivity Fault Management Mode | 71

erroneous-ccm

Syntax

```
erroneous-ccm;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the defect condition that raises an alarm indication signal when any cross-connect continuity check messages (CCMs) with an unexpected MEP ID or an erroneous maintenance domain level are received by the MEP.

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 | 286

Configuring ETH-AIS on a CFM MEP | 292

evc-protocol cfm

Syntax

```
evc-protocol cfm {
    maintenance-association association-name | vpls routing-instance routing-id;
    maintenance-domain domain-id;
    mep-id mep-id;
}
```

Hierarchy Level

[edit protocols oam **ethernet** evcs]

Release Information

Statement introduced in Junos OS Release 9.5.
mep-id *mep-id* statement introduced in Junos OS Release 15.1.

Description

Specify connectivity fault management (CFM) or virtual private LAN service (VPLS) as the Ethernet virtual connection (EVC) protocol.

Options

management-domain *domain-id*—(Optional) For CFM, specify the CFM management domain.

management-association *association-id*—(Optional) For CFM, specify the CFM management association.

routing-instance *instance-id*—(Optional) For VPLS, specify the VPLS routing instance.

mep-id *mep-id*—(Required for CFM) Identifier for the maintenance association endpoint

NOTE: This option is available on MX Series routers only.

Range: 1 through 8191

Required Privilege Level

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

RELATED DOCUMENTATION

lmi (Ethernet OAM)

event (CFM)

Syntax

```
    event {
        adjacency-loss;
        interface-status-tlv [lower-layer-down down];
        port-status-tlv blocked;
        rdi;
    }
}
```

Hierarchy Level

[edit protocols oam **ethernet** connectivity-fault-management **action-profile**]

Release Information
Statement introduced in Junos OS Release 10.1

Description
Configure threshold values for connectivity fault management events in an action profile.

Options
adjacency-loss—Connectivity is lost.

interface-status-tlv [lower-layer-down down]—Values that need to be monitored in interface status TLV.

port-status-tlv—Values that need to be monitored in port status TLV.

rdi—RDI received from some 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 CFM Action Profile to Specify CFM Actions for CFM Events | 65

interface-status-tlv | 1804

port-status-tlv | 1833

flap-trap-monitor

Syntax

```
flap-trap-monitor seconds;
```

Hierarchy Level

```
[edit logical-systems name protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles],
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]
[edit logical-systems name protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles profile-name avg-fd-twoway-threshold],
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profilesprofile-name avg-fd-twoway-threshold]
[edit logical-systems name protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles profile-name avg-ifdv-twoway-threshold],
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profilesprofile-name avg-ifdv-twoway-threshold]
[edit logical-systems name protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles profile-name avg-flr-forward-threshold],
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profilesprofile-nameavg-flr-forward-threshold ]
[edit logical-systems name protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles profile-name avg-flr-backward-threshold],
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profilesprofile-nameavg-flr-backward-threshold]
```

Release Information

Statement introduced in Junos OS Release 17.2R1 for MX Series routers.

Description

Enables damping of jnxSoamPmThresholdCrossingAlarm traps sent to the network management system (NMS) by summarizing the flap occurrences over a period of time and sends a single jnxSoamPmThresholdFlapAlarm notification to the NMS. You can enable damping at the global level for the iterator or you can enable damping at the individual threshold type of an iterator. You can specify the duration of time for summarizing flap occurrences.

Options

seconds—Duration in seconds, for summarizing flap occurrences and send out a single jnxSoamPm ThresholdFlapAlarm notification to the NMS.

Range: 1 through 360 seconds

Required Privilege Level
routing

RELATED DOCUMENTATION

- avg-fd-twoway-threshold | **1764**
- avg-ifdv-twoway-threshold | **1766**
- avg-flr-backward-threshold | **1770**
- avg-flr-forward-threshold | **1768**
- sla-iterator-profiles | **1847**
- Damping CFM performance Monitoring Traps and Notifications to Prevent Congestion of The NMS | **81**

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 | 166
- Guidelines for Configuring Routers to Support an ETH-DM Session | 186
- Enabling the Hardware-Assisted Timestamping Option | 198

hardware-assisted-keepalives

Syntax

```
hardware-assisted-keepalives [enable | disable];
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
```

Release Information

Statement introduced in Junos OS Release 14.2R1.

Description

For Ethernet interfaces on Modular Port Concentrators (MPCs) in MX Series routers only, delegate the transmission of the continuity check messages (CCMs) to the forwarding ASIC (that is, to the hardware) by enabling inline transmission of CCMs. Inline transmission of CCMs is also known as Inline-KA.

By default, CCMs are transmitted by the CPU of the MPC and not by the hardware. If the duration between transmissions of CCMs is low or if the CCMs for a specific line card scale, we recommend that you enable delegation of the transmission of CCMs to the hardware. By enabling inline transmission of CCMs, you can achieve maximum scaling of CCMs.

> **NOTE:** Starting in Junos OS Release 16.1R1, the inline support for 1s interval is supported on MPC1 to MPC7 (except MPC3 and MPC4) line cards.

Default

Inline transmission is disabled by default.

Options

enable—Enable inline transmission of CCMs.

> **NOTE:** Inline transmission of CCMs is not enabled when there is a CFM session already established. To enable inline transmission, you must first deactivate the CFM session using the **deactivate** command and then reactivate the CFM session using the **activate** command.

disable—Disable inline transmission of CCMs.

NOTE: After disabling inline transmission of CCMs, you must reboot the router for the changes to take effect.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Enabling Inline Transmission of Continuity Check Messages for Maximum Scaling | **301**

Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades | **75**

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 | 38

Configuring Continuity Check Protocol Parameters for Fault Detection | 39

instance

Syntax

```
instance vpls-instance-name;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain name]
```

Release Information

Statement introduced in Junos OS Release 9.4.

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) | 32

maintenance-domain | 1819

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 | 40

interface (OAM Link-Fault Management)

Syntax

```
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

```
[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-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 | 65

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

Statement introduced in Junos OS Release 9.6.

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 Port Status TLV and Interface Status TLV | 102

interface-status-send-rdi

Syntax

```
interface-status-send-rdi interface-status-send-rdi;
```

Hierarchy Level

[edit logical-systems *name* protocols **oam ethernet** connectivity-fault-management **maintenance-domain** *name* **maintenance-association** *name* **continuity-check**],
[edit protocols **oam ethernet** connectivity-fault-management **maintenance-domain** *name* **maintenance-association** *name* **continuity-check**]

Release Information

Statement introduced in Junos OS Release 17.3R1 for MX Series Routers.

Description

Configure CFM to propagate the status of the provider edge device via the remote defect indication (RDI) bit in the CC messages when the interface is down. When the status of the EVPN provider edge device is standby, the EVPN VPWS service is notified and it sets the interface status to CCC-down. When the interface status is CCC-down, it indicates that the provider edge service is down. When you enable CFM monitoring, CFM propagates the status of the provider edge device via the remote defect indication (RDI) bit in the CC messages. Thus, the customer edge device is aware that the provider edge device is down.

Usually, when the interface goes down, CFM propagates the status of the provider edge device via the interface status TLV. If the customer edge device does not support the interface status TLV, you can use the RDI bit to propagate the status of the provider edge device.

Required Privilege Level

routing—To view this statement in the configuration.

RELATED DOCUMENTATION

- interface-status-tlv | **1804**
- Configuring Port Status TLV and Interface Status TLV | **102**
- Understanding CFM Monitoring between CE and PE Devices | **101**

interval

Syntax

```
interval (100ms | 10m | 10ms | 10s | 1m | 1s| 3.3ms);
```

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.
Option **3.3ms** introduced in Junos OS Release 17.2.

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.

NOTE: When the continuity-check interval is set to 3.3ms, the actual interval is 4ms (250 pps).

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.

3.3ms—3.3 milliseconds.

Default: 1m

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 | 38

Configuring Continuity Check Protocol Parameters for Fault Detection | 39

Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades | 75

interval (CFM MEP)

Syntax

```
interval (1m | 1s);
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action
    log-and-generate-ais]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the interval between AIS messages that are to be received by the MEP as either 1 minute or 1 second.

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 | 286
Configuring ETH-AIS on a CFM MEP | 292

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 Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

sla-iterator-profile | **1845**

Configuring a Remote MEP with an Iterator Profile | **270**

iteration-period

Syntax

```
iteration-period iteration-period-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 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 | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

level

Syntax

level *number*;

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

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 | 31

level (CFM MEP)

Syntax

```
level value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action
    log-and-generate-ais]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the server maintenance domain level for the MEP.

Options

value—Maintenance domain level.

Range: 1 through 7

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 | 286

Configuring ETH-AIS on a CFM MEP | 292

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 | 51

log-and-generate-ais

Syntax

```
log-and-generate-ais {
    interval (1m | 1s);
    level level;
    priority level;
}
```

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management action-profile *action-profile-name* action]

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the action be taken when an AIS alarm is detected. The action includes generating and logging the AIS statistics along with the interval between AIS messages, the server maintenance domain level, and the priority of the AIS message.

Options

The other statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286

Configuring ETH-AIS on a CFM MEP | 292

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 | 38

Configuring Continuity Check Protocol Parameters for Fault Detection | 39

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 a MEP to Generate and Respond to CFM Protocol Messages | 40

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

RELATED DOCUMENTATION

Creating a Maintenance Association | 37

Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40

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;
            }
         }
      }
      mip-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 | 31
Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40

measurement-interval

Syntax

measurement-interval (5|15|30|60)

Hierarchy Level

[edit protocols oam ethernet cfm performance-monitoring]

[edit protocols oam ethernet cfm performance-monitoring sla-iterator-profiles *profile-name*]

Release Information

Description

Configure measurement interval to be used for a performance monitoring session. You must configure the measurement-interval at the **[edit protocols oam ethernet cfm performance-monitoring]** hierarchy level, which is a global level parameter. You can override the configured value by specifying a measurement-interval for the iterator profile at the **[edit protocols oam ethernet cfm performance-monitoring sla-taerator-profiles *profile-name*]** hierarchy level.

> **NOTE:** When you configure when MEF-36-compliant performance monitoring, you must also configure an **enhanced-sla-iterator** at the **[edit protocols oam ethernet cfm performance-monitoring]** hierarchy level.

Default

15 minutes

Required Privilege Level

configure—To enter configuration mode.
control—To modify any configuration.

RELATED DOCUMENTATION

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

Junos OS Support for Performance Monitoring Compliant with Technical Specification MEF 36 | 79

measurement-type

Syntax

```
measurement-type (loss | statistical-loss-measurement | two-way-delay);
```

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.
The **statistical-loss-measurement** option introduced in Junos OS Release 11.2.

Description

Configure the measurement type for the service level agreement (SLA) frames. An SLA frame is a type of packet used to measure frame loss in Ethernet connections.

Options

loss—Use Y.1731-compliant line module (LM) frames to measure frame loss.

statistical-loss-measurement— Use Y.1731-compliant two-way data module (DM) frames to statistically measure frame loss.

two-way-delay—Use Y.1731-compliant two-way DM frames to measure frame loss.

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

Configuring an Iterator Profile | 258

mep

Syntax

```
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 | 286

Configuring ETH-AIS on a CFM MEP | 292

Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40

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

Statement introduced in Junos OS Release 9.6.

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 | 31

maintenance-domain | 1819

name-format

Syntax

```
name-format (character-string | none | dns | mac+2oct);
```

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

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 | 37
Creating a Maintenance Domain | 31

no-aggregate-delegate-processing

Syntax

```
no-aggregate-delegate-processing;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Disable distribution of connectivity fault management (CFM) sessions on aggregated Ethernet interfaces.

Default

CFM sessions on aggregated Ethernet interfaces are distributed by default.

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

IEEE 802.1ag OAM Connectivity Fault Management Overview | 24

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 | 51

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 Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

Ethernet Frame Delay Measurements Overview | 166

Guidelines for Configuring Routers to Support an ETH-DM Session | 186

Enabling the Hardware-Assisted Timestamping Option | 198

policer (CFM Global)

Syntax

```
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 | 52

policer (CFM Session) | 1832

policer (CFM Session)

Syntax

```
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 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 | 52

policer (CFM Global) | 1831

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]
```

Release Information

Statement introduced in Junos OS Release 9.6.

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 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 | 65

Configuring Port Status TLV and Interface Status TLV | 102

priority (Protocols OAM)

Syntax

```
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 sla-iterator-profile profile-namesla-iterator-profile]
```

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Configure the priority of the iterator profile, which is the **vlan-pcp** value that is sent in the Y.1731 data frames.

Options

priority-value—Priority value, which is the **vlan-pcp** value that is sent in the Y.1731 data frames.

Range: 0 through 7

Default: 0

Required Privilege Level

Configure—To enter configuration mode.

Control—To modify any configuration.

RELATED DOCUMENTATION

sla-iterator-profile | 1845

Configuring a Remote MEP with an Iterator Profile | 270

priority (CFM MEP)

Syntax

```
priority value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action log-generate-ais]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the 802.1p priority of the AIS packet.

Options

value—Priority level.

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

Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286

Configuring ETH-AIS on a CFM MEP | 292

priority (OAM Connectivity-Fault Management)

Syntax

```
priority number;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-namemaintenance-association
    ma-name mep mep-id]
```

For EX Series Switches:

```
[edit protocols oam ethernet connectivity-fault-management
    maintenance-domaindomain-namemaintenance-association ma-name mepmep-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 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 | 40

protocol (Server MEP)

Syntax

```
protocol (l2circuit | l2vpn | ethernet) {
    interface interface-name;
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Configure the protocol as Layer 2 circuit, Layer 2 VPN, or Ethernet and associate the interface to the protocol that needs to be monitored for ETH-AIS.

Options

l2circuit—Configure the protocol for the server MEP as Layer 2 circuit.

l2vpn—Configure the protocol for the server MEP as Layer 2 VPN.

ethernet—Configure the protocol for the server MEP as Ethernet.

interface *interface-name*—The interface that is to be associated with the protocol that needs monitoring for ETH-AIS.

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 | 286

Configuring ETH-AIS on a CFM MEP | 292

protect-maintenance-association (OAM)

Syntax

```
protect-maintenance-association protect-ma-name;
```

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 11.4

Description

Configure the name of the protect transport path for the maintenance-association.

Options

protect-ma-name—The name of the protect transport path.

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 | 40

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 | 65

receive-ais

Syntax

```
receive-ais;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name event
    ais-trigger-condition]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Send a message to the peer MEPs when an AIS message is received by a peer MEP at its own maintenance level.

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 | 286
Configuring ETH-AIS on a CFM MEP | 292

remote-maintenance-association (OAM)

Syntax

```
remote-maintenance-association remote-ma-name;
```

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 11.4.

Description

Configure the name of the remote maintenance association.

Options

remote-ma-name—Name of the remote maintenance association.

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 | 40

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

```
[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 Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

Configuring a MEP to Generate and Respond to CFM Protocol Messages | 40

detect-loc | 1786

sendid-tlv

Syntax

```
sendid-tlv {
   send-chassis-tlv;
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
maintenance-domain-name maintenance-association maintenance-association-name
continuity-check]
```

Release Information

Statement introduced in Junos OS Release 16.1R2.

Description

Configures Junos OS to send the sender ID TLV along with the packets. The sender ID TLV is an optional TLV that is sent in continuity check messages (CCMs), loopback messages, and Link Trace Messages (LTMs), as specified in the IEEE 802.1ag standard. TLVs (type, length, and value) are described in the IEEE 802.1ag standard for Connectivity Fault Management (CFM) as a method of encoding variable-length and optional information in a protocol data unit (PDU).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Chassis ID TLV | 116

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 | 37

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" on page 270.

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 | 258
- Configuring a Remote MEP with an Iterator Profile | 270
- Verifying the Configuration of an Iterator Profile | 261
- Managing Iterator Statistics | 264

sla-iterator-profiles | 1847

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]
```

Release Information

Statement introduced in Junos OS Release 11.1.

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" on page 258.

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 | 258

Configuring a Remote MEP with an Iterator Profile | 270

Verifying the Configuration of an Iterator Profile | 261

Managing Iterator Statistics | 264

CHAPTER 61

Configuration Statements: Ethernet OAM Link Fault Management

IN THIS CHAPTER

- action (OAM LFM) | **1851**
- action (OAM) | **1852**
- action-profile (Applying to OAM CFM, for EX Series Switch Only) | **1853**
- action-profile | **1855**
- age | **1857**
- allow-remote-loopback | **1858**
- apply-action-profile | **1859**
- auto-discovery (EX Series Switch Only) | **1860**
- calculation-weight | **1861**
- connectivity-fault-management (EX Series Switch Only) | **1862**
- continuity-check (EX Series Switch Only) | **1864**
- cycle-time | **1865**
- delay | **1866**
- delay-variation | **1867**
- ethernet (Protocols OAM) | **1868**
- event (LFM) | **1876**
- event-thresholds | **1878**
- event-thresholds | **1879**
- fast-aps-switch | **1880**
- frame-error | **1881**
- frame-period | **1882**
- frame-period | **1883**
- frame-period-summary | **1884**
- frame-period-summary | **1885**
- hold-interval (OAM CFM, for EX Series Switch Only) | **1886**
- hold-interval (OAM) | **1887**
- interface (OAM CFM, for EX Series Switch Only) | **1888**

- interface (OAM Link-Fault Management) | **1889**
- interval (EX Series Switch Only) | **1890**
- iteration-period | **1891**
- level (EX Series Switch Only) | **1892**
- link-adjacency-loss | **1893**
- link-discovery | **1894**
- link-down | **1895**
- link-event-rate | **1896**
- link-fault-management | **1897**
- negotiation-options | **1899**
- no-allow-link-events | **1900**
- oam | **1901**
- path-database-size (EX Series Switch Only) | **1905**
- pdu-interval | **1906**
- pdu-threshold | **1907**
- performance-monitoring (OAM LFM) | **1908**
- protocol-down | **1909**
- protocol-down | **1910**
- remote-loopback | **1911**
- remote-mep (EX Series Switch Only) | **1912**
- send-critical-event | **1913**
- sla-iterator-profiles (OAM CFM) | **1914**
- symbol-period | **1915**
- syslog (OAM Action) | **1916**
- traceoptions (Individual Interfaces) | **1917**
- version-ipfix (Services) | **1926**

action (OAM LFM)

Syntax

```
action {
   syslog;
   link-down;
}
```

Hierarchy Level

```
[edit protocols oam ethernet link-fault-management]
```

Release Information

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

Description

Define the action or actions to be taken when the OAM link fault management (LFM) fault event occurs.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

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 | 150

action-profile (Applying to OAM CFM, for EX Series Switch Only)

Syntax

```
action-profile profile-name {
    action {
        interface-down;
    }
    default-actions {
        interface-down;
    }
    event {
        adjacency-loss;
    }
}
```

Hierarchy Level

[edit protocols **oam ethernet connectivity-fault-management**]

[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 10.2 for EX Series switches.

Description

Configure a name and default action for an action profile.

Options

profile-name—Name of the action profile.

action—Defines the action to be taken when connectivity to the remote MEP is lost.

interface-down—Brings the interface down when a remote MEP connectivity failure. is detected.

default-actions—Defines the default action to be taken when connectivity to the remote MEP is lost.

interface-down—Brings the interface down when a remote MEP connectivity failure is detected.

event—Defines the event to be monitored when a remote MEP connectivity failure is detected.

adjacency-loss—Defines the connectivity loss to the remote MEP.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

action-profile

List of Syntax

Syntax: T, M, MX and ACX Series Routers, SRX Series Firewalls and EX Series Switches on page 1855
Syntax: EX Series Switches and NFX Series Devices on page 1855

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 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 an OAM Action Profile | **149**

Configuring Ethernet OAM Link Fault Management | **329**

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 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 | 51

allow-remote-loopback

Syntax

```
allow-remote-loopback;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management interface** *interface-name*]

Release Information

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

Description

Advertise that the interface is capable of getting into loopback mode. Enable remote loopback in Ethernet OAM link fault management (LFM) on all Ethernet interfaces or the specified interface on the EX Series switch.

WARNING: If you disable this statement on a peer interface, LFM loopback enable and disable commands will not work. Before disabling this configuration, please make sure the remote-loopback interface is disabled.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Ethernet OAM Link Fault Management | 331
Configuring Ethernet OAM Link Fault Management | 329

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 | 153

auto-discovery (EX Series Switch Only)

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 10.2 for EX Series switches.

Description

Enable the MEP to accept continuity check messages from all remote MEPs.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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 | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- delay | 1783
- delay-variation | 1785

connectivity-fault-management (EX Series Switch Only)

Syntax

```
connectivity-fault-management {
  action-profile profile-name {
    action {
      interface-down;
    }
    default-actions {
      interface-down;
    }
    event {
      adjacency-loss;
    }
  }
  linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
  }
  maintenance-domain 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;
        remote-mep mep-id {
          action-profile profile-name;
        }
      }
    }
  }
  performance-monitoring {
    sla-iterator-profiles {
      profile-name {
```

```
            calculation-weight {
               delay delay-value;
               delay-variation delay-variation-value;
            }
            cycle-time cycle-time-value;
            iteration-period iteration-period-value;
            measurement-type two-way-delay;
            passive;
         }
      }
   }
}
```

Hierarchy Level

```
[edit protocols oam ethernet]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.
performance-monitoring introduced in Junos OS Release 11.4 for EX Series switches.

Description

Configure connectivity fault management for IEEE 802.1ag Operation, Administration, and Management (OAM) support.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

continuity-check (EX Series Switch Only)

Syntax

```
continuity-check {
    hold-interval minutes;
    interface-status-tlv;
    interval (10m | 10s | 1m | 1s| 100ms);
    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 10.2 for EX Series switches.

Description

Specify continuity check protocol options.

The remaining statements are explained separately. See CLI Explorer.

Options

interface-status-tlv—Includes interface status TLV in CCM.

port-status-tlv—Includes port status TLV in CCM.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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 Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

Configuring an Iterator Profile | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

delay

Syntax

```
delay delay-value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name calculation-weight]
```

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.

Options

delay-value—Calculation weight for delay.

> **NOTE:** This option is applicable only for two-way delay measurement.

Range: 1 through 65,535

Default: 1

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

- Configuring an Iterator Profile | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- calculation-weight | 1772

delay-variation

Syntax

```
delay-variation delay-variation-value;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles
    profile-name calculation-weight]
```

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 variation.

Options

delay-variation-value—Calculation weight for delay variation.

> **NOTE:** This option is applicable only for two-way delay measurement.

Range: 1 through 65,535

Default: 1

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

RELATED DOCUMENTATION

- Configuring an Iterator Profile | 258
- Configuring an Iterator Profile on a Switch (CLI Procedure) | 341
- calculation-weight | 1772

ethernet (Protocols OAM)

List of Syntax

Syntax: MX, T, ACX Series Routers, SRX Firewalls, M320 and EX Series Switches on page 1868
Syntax: EX Series Switches and NFX Series Devices on page 1872

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-evc;
                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 {
     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-errorcount;
            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 | 331

event (LFM)

List of Syntax

Syntax: MX, M, T, ACX Series Routers, SRX Firewalls and EX Series Switches on page 1876
Syntax: EX Series Switches and NFX Series Devices on page 1876

Syntax: MX, M, T, ACX Series Routers, SRX Firewalls and EX Series Switches

```
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

```
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 | 152
Configuring Ethernet OAM Link Fault Management | 329

event-thresholds

Syntax

```
event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management interface** *interface-name*]

Release Information

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

Description

Configure threshold limit values for link events in periodic OAM PDUs.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

event-thresholds

Syntax

```
event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

Hierarchy Level

```
[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 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 | 138

fast-aps-switch

Syntax

```
fast-aps-switch;
```

Hierarchy Level

```
[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

frame-error

Syntax

```
frame-error count;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management event link-event-rate**],
[edit protocols **oam ethernet link-fault-management interface** *interface-name* **event-thresholds**]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Configure the threshold value for sending frame error events or taking the action specified in the action profile.

Frame errors occur on the underlying physical layer. The threshold is reached when the number of frame errors reaches the configured value.

Options
count—Threshold count in seconds for frame error events.
Range: 1 through 100 seconds
Default: 1 second

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

frame-period

Syntax

```
frame-period count;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management event link-event-rate**],
[edit protocols **oam ethernet link-fault-management interface** *interface-name* **event-thresholds**]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Configure the number of frame errors within the last N frames that has exceeded a threshold.

Frame errors occur on the underlying physical layer. The threshold is reached when the number of frame errors reaches the configured value.

Options
count—Threshold count in seconds for frame error events.
Range: 1 through 100 seconds

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

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 | 138
Configuring Threshold Values for Fault Events in an Action Profile | 153

frame-period-summary

Syntax

```
frame-period-summary count;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management event link-event-rate**],
[edit protocols **oam ethernet link-fault-management interface** *interface-name* **event-thresholds**]

Release Information

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

Description

Configure the threshold value 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.

Options

count—Threshold count in seconds for frame period summary error events.

Range: 1 through 100 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

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 | 138

Configuring Threshold Values for Fault Events in an Action Profile | 153

hold-interval (OAM CFM, for EX Series Switch Only)

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 10.2 for EX Series switches.

Description

Configure the time to wait before flushing the maintenance association end point (MEP) database, if no updates occur.

Options

minutes—Time to wait, in minutes.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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 | 38

Configuring Continuity Check Protocol Parameters for Fault Detection | 39

interface (OAM CFM, for EX Series Switch Only)

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 10.2 for EX Series switches.

Description

Configure IEEE 802.1ag Operation, Administration, and Management (OAM) Connectivity Fault Management (CFM) support for the specified interface.

Options

interface-name—Interface to which the MEP is attached. It can be a physical Ethernet interface or a logical interface. If the interface is a trunk interface, the VLAN associated with the interface must have a VLAN ID.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

interface (OAM Link-Fault Management)

Syntax

```
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

```
[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

interval (EX Series Switch Only)

Syntax

```
interval (10m | 10s | 1m | 1s | 100ms | 10ms);
```

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 10.2 for EX Series switches.

Description
Configure the time between continuity check messages.

Options
10m—10 minutes.

10s—10 seconds.

1m—1 minute.

1s—1 second.

100ms—100 milliseconds.

10ms—10 milliseconds.

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

iteration-period

Syntax

```
iteration-period iteration-period-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 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 | 258

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

level (EX Series Switch Only)

Syntax

```
level number;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
```

Release Information

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

Description

Configure a number to be used in CFM messages to identify the maintenance association.

Options

number—Number used to identify the maintenance domain to which the CFM message belongs.

Range: 0 through 7

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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 9.4 for EX Series switches.

Description

Configure **loss of adjacency** event with the IEEE 802.3ah link fault management (LFM) peer. When included, the loss of adjacency event triggers the action specified under the **action** statement.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Ethernet OAM Link Fault Management | **331**

Configuring Ethernet OAM Link Fault Management | **329**

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 9.4 for EX Series switches.

Description
Specify the discovery mode used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support. The discovery process is triggered automatically when OAM 802.3ah functionality is enabled on an interface. Link monitoring is done when the interface sends periodic OAM PDUs.

Options
active—In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality.

passive—In passive mode, the peer initiates the discovery process.

Once the discovery process is initiated, both sides participate in discovery.

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

link-down

Syntax

```
link-down;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management action-profile action**]

Release Information

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

Description

Mark the interface as down for transit traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | **329**

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 9.4 for EX Series switches.

Description

Configure the number of link fault management (LFM) events per second.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

link-fault-management

Syntax

```
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-errorcount;
            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 9.4 for EX Series switches.

Description

Configure Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Ethernet OAM Link Fault Management | 331

Configuring Ethernet OAM Link Fault Management | 329

negotiation-options

Syntax

```
negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
}
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management interface** *interface-name*]

Release Information

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

Description

Enable and disable IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) features for Ethernet interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

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 9.4 for EX Series switches.

Description

Disable the sending of link event TLVs.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

oam

Syntax

```
oam {
  ethernet{
    connectivity-fault-management {
      action-profile profile-name {
        action {
          interface-down;
        }
        default-actions {
          interface-down;
        }
        event {
          adjacency-loss;
        }
      }
      linktrace {
        age (30m | 10m | 1m | 30s | 10s);
        path-database-size path-database-size;
      }
      maintenance-domain 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;
            remote-mep mep-id {
              action-profile profile-name;
            }
          }
        }
      }
      performance-monitoring {
```

```
        sla-iterator-profiles {
            profile-name {
                calculation-weight {
                    delay delay-value;
                    delay-variation delay-variation-value;
                }
                cycle-time cycle-time-value;
                iteration-period iteration-period-value;
                measurement-type two-way-delay;
                passive;
            }
        }
    }
}
```

```
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-errorcount;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
        negotiation-options {
            allow-remote-loopback;
            no-allow-link-events;
        }
    }
  }
}
```

Hierarchy Level

[edit protocols]

Release Information

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

connectivity-fault-management introduced in Junos OS Release 10.2 for EX Series switches.

Description

Provide IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support for Ethernet interfaces on EX Series switches or configure connectivity fault management (CFM) for IEEE 802.1ag Operation, Administration, and Management (OAM) support on the switches.

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

- Example: Configuring Ethernet OAM Link Fault Management | 331
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches | 315
- Configuring Ethernet OAM Link Fault Management | 329
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

path-database-size (EX Series Switch Only)

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 10.2 for EX Series switches.

Description

Specify the number of linktrace reply entries to be stored per linktrace request.

Options

path-database-size—Database size (number of entries stored per request).

Range: 1 through 500

Default: 100

Required Privilege Level

routing—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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: 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 | 138
- Example: Configuring Ethernet OAM Link Fault Management | 331
- Configuring Ethernet OAM Link Fault Management | 329

pdu-threshold

Syntax

```
pdu-threshold threshold-value;
```

Hierarchy Level

```
[edit protocols oam ethernet link-fault-management interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 8.2 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 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 | 138

Configuring Ethernet OAM Link Fault Management | 329

performance-monitoring (OAM LFM)

Syntax

```
performance-monitoring {
   sla-iterator-profiles {
      profile-name {
         calculation-weight {
            delay delay-value;
            delay-variation delay-variation-value;
         }
         cycle-time cycle-time-value;
         iteration-period iteration-period-value;
         measurement-type two-way-delay;
         passive;
      }
   }
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description

Specify performance monitoring support for Ethernet frame 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 MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) | 339
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 340
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) | 343

protocol-down

Syntax

```
protocol-down;
```

Hierarchy Level

```
[edit protocols oam ethernet link-fault-management event]
```

Release Information

Statement introduced in JUNOS Release 9.4 for EX-series switches.

Description

Configure the upper layer indication of a 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

Example: Configuring Ethernet OAM Link Fault Management | 331
Configuring Ethernet OAM Link Fault Management | 329

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 | 149

remote-loopback

Syntax

```
remote-loopback;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management interface** *interface-name*]

Release Information

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

Description

Set the data terminal equipment (DTE) in loopback mode. Remove the statement from the configuration to take the DTE out of loopback mode. It is used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Ethernet OAM Link Fault Management | 331
Configuring Ethernet OAM Link Fault Management | 329

remote-mep (EX Series Switch Only)

Syntax

```
remote-mep mep-id {
    action-profile profile-name;
}
```

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 10.2 for EX Series switches.

Description

Specify the numeric identifier of the remote maintenance association end point (MEP) within the maintenance association.

Options

mep-id—Specify the numeric identifier of the MEP.

Range: 1 through 8191

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.

RELATED DOCUMENTATION

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) | 320

Junos OS Network Interfaces Configuration Guide

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 | **150**

sla-iterator-profiles (OAM CFM)

Syntax

```
sla-iterator-profiles {
    profile-name {
        calculation-weight {
            delay delay-value;
            delay-variation delay-variation-value;
        }
        cycle-time cycle-time-value;
        iteration-period iteration-period-value;
        measurement-type two-way-delay;
        passive;
    }
}
```

Hierarchy Level

[edit protocols **oam ethernet connectivity-fault-management performance-monitoring**]

Release Information

Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description

Configure an iterator application and specify the iterator profile options.

Options

profile-name—Name of the 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 on a Switch (CLI Procedure) | 341

symbol-period

Syntax

```
symbol-period count;
```

Hierarchy Level

[edit protocols **oam ethernet link-fault-management action-profile**; **event link-event-rate**] ,
[edit protocols **oam ethernet link-fault-management interface** *interface-name* **event-thresholds**]

Release Information

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

Description

Configure the threshold for sending symbol period events or taking the action specified in the action profile.

Symbol code errors occur on the underlying physical layer. The symbol period threshold is reached when the number of symbol errors reaches the configured value within the period. You cannot configure the default value to a different value.

Options

count—Threshold count in seconds for symbol period events.

Range: 1 through 100 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Ethernet OAM Link Fault Management | 329

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 | 150

Configuring Ethernet OAM Link Fault Management | 329

traceoptions (Individual Interfaces)

List of Syntax

Syntax (Individual interfaces with PTX Series, EX Series, ACX Series) on page 1917
Syntax (Individual interfaces with QFX Series, OCX1100, EX4600, NFX Series) on page 1917
Syntax (OAMLFM with EX Series, QFX Series, NFX Series) on page 1917
Syntax (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series) on page 1917

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 207 on page 1920 lists options for traceoption command for the following platforms:

Table 207: Options for traceoptions

Option	Individual interfaces with PTX Series, ACX Series, EX Series	Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series	Interface Process with OAMLFM with EX Series, QFX Series, NFX Series	Interface process with ACX Series, SRX Series, MX Series, M Series, T Series
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/dcd*** . By default, interface process tracing output is placed in the file.		—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/dcd*** .	—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/dcd*** . By default, interface process tracing output is placed in the file **dcd**.
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.		—(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 *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.	—(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

Table 207: Options for traceoptions *(continued)*

Option	Individual interfaces with PTX Series, ACX Series, EX Series	Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series	Interface Process with OAMLFM with EX Series, QFX Series, NFX Series	Interface process with ACX Series, SRX Series, MX Series, M Series, T Series
				1000 *Default:* 3 files
flag	—Tracing operation to perform. To specify more than one tracing operation, include multiple ***flag*** statements. The following are the interface-specific tracing options. • **all**—All interface tracing operations • **event**—Interface events • **ipc**—Interface interprocess communication (IPC) messages • **media**—Interface media changes • **q921**—Trace ISDN Q.921 frames • **q931**—Trace ISDN Q.931 frames	—Tracing operation to perform. To specify more than one tracing operation, include multiple ***flag*** statements. The following are the interface-specific tracing options. • **all**—All interface tracing operations • **event**—Interface events • **ipc**—Interface interprocess communication (IPC) messages • **media**—Interface media changes • **q921**—Trace ISDN Q.921 frames • **q931**—Trace ISDN Q.931 frames	—Tracing operation to perform. To specify more than one tracing operation, include multiple ***flag*** statements. You can include the following flags: • **action-profile**—Trace action profile invocation events. • **all**—Trace all events. • **configuration**—Trace configuration events. • **protocol**—Trace protocol processing events. • **routing socket**—Trace routing socket events.	—Tracing operation to perform. To specify more than one tracing operation, include multiple ***flag*** statements. You can include the following flags: • **all** • **change-events**—Log changes that produce configuration events • **config-states**—Log the configuration state machine changes • **kernel**—Log configuration IPC messages to kernel • **kernel-detail**—Log details of configuration messages to kernel
match	—(Optional) Regular expression for lines to be traced.		—(Optional) Refine the output to log only those lines that match the given regular expression.	

Table 207: Options for traceoptions *(continued)*

Option	Individual interfaces with PTX Series, ACX Series, EX Series	Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series	Interface Process with OAMLFM with EX Series, QFX Series, NFX Series	Interface process with ACX Series, SRX Series, MX Series, M Series, T Series
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.		—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the files option. *Syntax:* *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB *Range:* 10 KB through 1 GB *Default:* 128 KB *Default:* If you do not include this option, tracing output is appended to an existing trace file.	

Table 207: Options for traceoptions *(continued)*

Option	Individual interfaces with PTX Series, ACX Series, EX Series	Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series	Interface Process with OAMLFM with EX Series, QFX Series, NFX Series	Interface process with ACX Series, SRX Series, MX Series, M Series, T Series
				—(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

Table 207: Options for traceoptions *(continued)*

Option	Individual interfaces with PTX Series, ACX Series, EX Series	Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series	Interface Process with OAMLFM with EX Series, QFX Series, NFX Series	Interface process with ACX Series, SRX Series, MX Series, M Series, T Series
				supported on your router *Default:* 1 MB
no-world-readable	—(Optional) Prevent any user from reading the log file.		—(Optional) Restrict file access to the user who created the file.	—(Optional) Disallow any user to read the log file.
world-readable	—(Optional) Allow any user to read the log file.		—(Optional) Enable unrestricted file access.	—(Optional) Allow any user to read the log file.
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**.
no-remote-trace			—(Optional) Disable the remote trace.	-
match *regex*				—(Optional) Refine the output to include only those lines that match the given regular expression.

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

Tracing Operations of an Individual Router or Switch Interface

Example: Configuring Ethernet OAM Link Fault Management | **331**

Configuring Ethernet OAM Link Fault Management | **329**

Tracing Operations of the Interface Process

version-ipfix (Services)

Syntax

```
version-ipfix {
    template template-name {
        flow-active-timeout seconds;
        flow-inactive-timeout seconds;
        flow-key {
            flow-direction;
            vlan-id;
            output-interface;
        }
        (ipv4-template | ipv6-template | mpls-ipv4-template | mpls-ipvx-template | vpls-template);
        nexthop-learning (enable |disable);
        observation-domain-id
        option-refresh-rate packets packets seconds seconds;
        options-template-id
        template-id
        template-refresh-rate packets packets seconds seconds;
        tunnel-observation [ipv4 | ipv6 | mpls-over-udp];
    }
}
```

Hierarchy Level

```
[edit services flow-monitoring]
```

Release Information

Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.R3 for EX Series switches.
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed.
Statement introduced in Junos OS Release 17.2R1 for QFX10002 switches.
Statement introduced in Junos OS Release 17.4R1 for QFX10008 and QFX10016 switches.

Description

Specify the IPFIX output template properties to support flow monitoring.

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 Inline Active Flow Monitoring Using Routers, Switches or NFX250*
- *Configuring Inline J-Flow to Use IPFIX Flow Templates on MX, vMX and T Series Routers, EX Series Switches and NFX250, and SRX Devices*
- *Configuring Inline Active Flow Monitoring on PTX Series Routers*

CHAPTER 62

Configuration Statements: sFlow Technology

IN THIS CHAPTER

- adaptive-sample-rate | **1929**
- agent-id | **1931**
- collector | **1932**
- disable (sFlow Monitoring Technology) | **1934**
- disable-sw-rate-limiter | **1935**
- interfaces (sFlow) | **1936**
- polling-interval | **1938**
- sample-rate | **1940**
- sample-rate (QFX Series) | **1942**
- sflow | **1943**
- source-ip | **1947**
- traceoptions (sFlow Technology) | **1948**
- udp-port | **1950**
- udp-port (QFX Series) | **1951**

adaptive-sample-rate

Syntax

```
adaptive-sample-rate rate {
    fallback;
    sample-limit-threshold sample-limit-threshold;
}
```

Hierarchy Level

[edit protocols sflow]

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.
Statement introduced in Junos OS Release 18.3R1 for QFX Series switches.
adaptive-sample-rate limit is increased in Junos OS Release 19.1R1.

Description

Configure and back up the adaptive sampling rate in sFlow monitoring technology configurations.

Routers and switches use adaptive sampling to ensure both sampling accuracy and efficiency. Adaptive sampling is a process of monitoring the overall incoming traffic rate on the network device and providing intelligent feedback to interfaces to dynamically adapt the sampling rates on interfaces on the basis of traffic conditions.

Default

sFlow technology is disabled by default.

Options

rate—Configure the maximum number of samples that should be generated per line card.

Range: 300 through 9500 pps

fallback—Enable adaptive sampling fallback (also called reverse adaptive sampling).

sample-limit-threshold—Explicitly specify the threshold value in packets per second (pps) for each line card.

You must configure the **fallback** statement to be able to configure the **sample-limit-threshold** statement.

Range: 0 through 4750 pps.

Required Privilege Level

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

RELATED DOCUMENTATION

sflow | 1943

show sflow interface | 2628

Understanding How to Use sFlow Technology for Network Monitoring | 975

Example: Monitoring Network Traffic Using sFlow Technology | 999

agent-id

List of Syntax

Syntax (EX Series) on page 1931
Syntax (MX Series, QFX Series, OCX Series, and PTX Series) on page 1931

Syntax (EX Series)

```
agent-id ip-address;
```

Syntax (MX Series, QFX Series, OCX Series, and PTX Series)

```
agent-id {
    ipv4-address;
    inet6 ipv6-address;
}
```

Hierarchy Level

```
[edit protocols sflow]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.
Support for IPv6 addresses introduced in Junos OS Release 19.1R1 for MX Series, PTX Series, and QFX Series devices.

Description

Configure the IP address to be assigned as the agent ID for the sFlow agent. By assigning an IP address, you ensure that the IP address is not dynamic. You can specify an IPv4 or IPv6 address or both.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

collector

List of Syntax

Syntax (EX Series) on page 1932
Syntax (ACX Series, MX Series, OCX Series, PTX Series, and QFX Series) on page 1932

Syntax (EX Series)

```
collector ip-v4/v6-address {
    udp-port port-number;
}
```

Syntax (ACX Series, MX Series, OCX Series, PTX Series, and QFX Series)

```
collector ip-v4/v6-address {
    dscp dscp;
    forwarding-class forwarding-class;
    udp-port port-number;
}
```

Hierarchy Level

```
[edit protocols sflow]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.
dscp and **forwarding-class** options introduced in Junos OS Release 19.1R1, for PTX Series routers and QFX Series switches (previously introduced for MX Series routers).

Description

Configure a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to this collector for analysis. You can configure up to four collectors on the device. You configure a collector by specifying its IP address and a UDP port.

Options

dscp ***dscp***—Configure Differentiated Services Code Point (DSCP) values per collector. These values are applied to all the packets destined for that collector. A change in the DSCP configuration resets all the counters for the collector and the new configuration comes into effect.

forwarding-class ***forwarding-class***—Configure forwarding class values per collector. These values are applied to all the packets destined for that collector. A change in the forwarding-class configuration does not reset the counters. The collector maintains its state and the new configuration comes into effect.

ip-address (*ipv4-address* | *ipv6-address*)—Configure the IP address.

(*ipv4-address* | *ipv6-address*) —(EX Series only) Set the IPv4 or IPv6 address.

udp-port ***port-number***—Configure the collector UDP port number.

Default: 6343

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**

disable (sFlow Monitoring Technology)

Syntax

```
disable;
```

Hierarchy Level

[edit protocols **sflow**],
[edit protocols **sflow interfaces** *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.

Description

Disable the sFlow monitoring protocol on all interfaces on the switch or on the specified interface.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**
- Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**

disable-sw-rate-limiter

Syntax

```
disable-sw-rate-limiter;
```

Hierarchy Level

```
[edit protocols sflow]
```

Release Information

Statement introduced in Junos OS Release 17.2R1 for QFX10000 Series switches.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.

Description

Configure the sFlow sampling rate to stay within the maximum accurate sampling rate: In sFlow, packet-based sampling is implemented in the hardware, so that all the interfaces can be monitored with very little overhead. However, if traffic levels are unusually high, the hardware generates more samples than it can handle. The extra samples are dropped by the software rate-limiting algorithm and can cause inaccurate results. Enabling the **disable-sw-rate-limiter** statement disables the software rate-limiting algorithm and allows the hardware sampling rate to stay within the maximum sampling rate.

Packet-based sampling samples one packet out of a specified number of packets from an interface enabled for sFlow. The sampling rate is a fraction in the form 1/*N*, meaning that, on average, one out of every N packets will be sampled:

- QFX10000 switches support a maximum sampling rate of 1 out of 65,536 packets. A rate of 5,000 samples per line card is supported on QFX10000 Series switches for sFlow technology.
- PTX routers support a maximum sampling rate of 1 out of 64K packets.

Required Privilege Level

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

interfaces (sFlow)

List of Syntax

Syntax: ACX Routers, OCX1100, EX4600 and QFX Switches on page 1936
Syntax: EX Series Switches, PTX Routers on page 1936

Syntax: ACX Routers, OCX1100, EX4600 and QFX Switches

```
interfaces interface-name {
    polling-interval seconds;
    sample-rate number;
}
```

Syntax: EX Series Switches, PTX Routers

```
interfaces interface-name {
    polling-interval seconds;
    sample-rate {
        egress number;
        ingress number;
    }
}
```

Hierarchy Level

```
[edit protocols sflow]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.

Description

Configure sFlow network traffic monitoring on the specified interface on the device. You can configure sFlow parameters such as polling interval and sampling rate with different values on different interfaces, and you can also disable sFlow monitoring on individual interfaces.

The remaining statements are explained separately. See CLI Explorer.

Options

interface-name—Name of the interface on which to configure sFlow parameters.

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

RELATED DOCUMENTATION

- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**
- Example: Monitoring Network Traffic Using sFlow Technology | **999**
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**
- Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**

polling-interval

Syntax

```
polling-interval seconds;
```

Hierarchy Level

```
[edit protocols sflow],
[edit protocols sflow interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.

Description

Configure the interval (in seconds) that the device waits between port statistics update messages. *Polling* refers to the device successively gathering various statistics for the network interfaces configured for sFlow monitoring and exporting the statistics to the configured sFlow collector.

Default

If no polling interval is configured for a particular interface, the device uses the global polling interval configured at the **[edit protocols sflow]** hierarchy level. If no global interval is configured, the device uses the default polling interval of 20 seconds.

Options

seconds—Number of seconds between successive samples of interface statistics. Specifying a value of 0 (zero) disables the polling.

Range: 0 through 3600 seconds

Default: 20 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Example: Monitoring Network Traffic Using sFlow Technology | 999

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | 985

Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | 990

sample-rate

Syntax

```
sample-rate {
    egress number;
    ingress number;
}
```

Hierarchy Level

```
[edit protocols sflow],
[edit protocols sflow interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
The option *number* (which immediately followed **sample-rate**) is no longer available and options **egress *number*** and **ingress *number*** added in Junos OS Release 10.4 for EX Series switches.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.

Description

Specify the number of egress or ingress packets out of which one packet is sampled. If no interface sampling rates are configured, the global sampling rates take effect. If neither is configured, by default both ingress and egress packet sampling are disabled.

Default

By default, both egress and ingress sampling rates are disabled.

Options

egress *number*—Value for egress sampling rate.

Range: 1 through 1,073,741,823

ingress *number*—Value for ingress sampling rate.

Range: 1 through 1,073,741,823

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | 985

sample-rate (QFX Series)

Syntax

```
sample-rate number;
```

Hierarchy Level

```
[edit protocols sflow],
[edit protocols sflow interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Specify the denominator (***number***) of the ratio that is the sample rate in sFlow traffic monitoring. For example, to configure a sample rate of 1 in 1000 packets, you specify a *number* of 1000.

Default

If no sample rate is configured for a particular interface, the device uses the global sample rate configured at the **[edit protocols sflow]** hierarchy level. If no global rate is configured, the device uses the default sample rate of 1 in 2000 packets.

Options

number—Denominator of the ratio representing the sample rate (one packet out of ***number***).

Range: 1 through 16,777,215

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

Example: Monitoring Network Traffic Using sFlow Technology | **999**

sflow

List of Syntax

Syntax (EX Series) on page 1943
Syntax (MX Series and EX92xx) on page 1943
Syntax (PTX Series, QFX Series, OCX Series, ACX Series, and EX4600) on page 1945

Syntax (EX Series)

```
sflow {
    adaptive-sample-rate rate {
        fallback;
        sample-limit-threshold sample-limit-threshold;
    }
    agent-id {
        ipv4-address;
        inet6 ipv6-address;
    }
    collector ip-v4/v6-address {
        udp-port port-number;
    }
    ;
    interfaces interface-name {
        polling-interval seconds;
        sample-rate {
            egress rate;
            ingress rate;
        }
    }
    polling-interval seconds;
    sample-rate {
        egress rate;
        ingress rate;
    }
    source-ip {
        ipv4-address;
        inet6 ipv6-address;
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag;
    }
}
```

Syntax (MX Series and EX92xx)

```
sflow {
    adaptive-sample-rate rate {
        fallback;
        sample-limit-threshold sample-limit-threshold;
    }
    agent-id {
        ipv4-address;
        inet6 ipv6-address;
    }
    collector ip-v4/v6-address {
        dscp dscp;
        forwarding-class forwarding-class;
        udp-port port-number;
    }
    inline-sampling;
    interfaces interface-name {
        polling-interval seconds;
        sample-rate {
            egress rate;
            ingress rate;
        }
    }
    polling-interval seconds;
    sample-rate {
        egress rate;
        ingress rate;
    }
    source-ip {
        ipv4-address;
        inet6 ipv6-address;
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag;
    }
}
```

Syntax (PTX Series, QFX Series, OCX Series, ACX Series, and EX4600)

```
sflow {
    adaptive-sample-rate rate {
        fallback;
        sample-limit-threshold sample-limit-threshold;
    }
    agent-id {
        ipv4-address;
        inet6 ipv6-address;
    }
    collector ip-v4/v6-address {
        dscp dscp;
        forwarding-class forwarding-class;
        udp-port port-number;
    }
    disable-sw-rate-limiter;
    ;
    interfaces interface-name {
        polling-interval seconds;
        sample-rate {
            egress number;
            ingress number;
        }
    }
    polling-interval seconds;
    sample-rate {
        egress number;
        ingress number;
    }
    source-ip {
        ipv4-address;
        inet6 ipv6-address;
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag;
    }
}
```

Hierarchy Level

```
[edit protocols]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.
dscp and **forwarding-class** options introduced in Junos OS Release 19.1R1, for PTX routers and QFX switches (previously introduced for MX Series).

Description

Configure sFlow technology to continuously monitor traffic at wire speed on specified interfaces simultaneously. sFlow data can be used to provide network traffic visibility information.

Default

sFlow technology is disabled by default.

Options

inline-sampling—Enables the sflow samples to be generated inline directly from packet fowarding engine.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding How to Use sFlow Technology for Network Monitoring | **975**

Understanding Inline Active Flow Monitoring

source-ip

List of Syntax

Syntax (EX Series) on page 1947
Syntax (MX Series, QFX Series, OCX Series, and PTX Series) on page 1947

Syntax (EX Series)

```
source-ip (ip4-address | ipv6-address);
```

Syntax (MX Series, QFX Series, OCX Series, and PTX Series)

```
source-ip {
    ipv4-address;
    inet6 ipv6-address;
}
```

Hierarchy Level

```
[edit protocols sflow]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.
IPv6 addresses are supported in Junos OS Release 19.1R1 for MX Series, PTX Series, and QFX Series devices

Description

Configure the IP address to be used for the sFlow datagrams. By configuring an IP address, you ensure that the IP address is not dynamic. You can specify an IPv4 or IPv6 address or both.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

traceoptions (sFlow Technology)

Syntax

```
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

[edit protocols sflow]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Define tracing operations for sFlow technology.

Default

The traceoptions feature is disabled.

Options

file *filename*—Name of the file to receive the tracing operation output. Enclose the name in quotation marks. Output files are located in the **/var/log/** directory.

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**. Incoming trace file data is logged in the now empty **trace-file**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify the maximum number of files, you must also specify the maximum file size using the **size** option.

Range: 2 through 1000 files

Default: 1 trace file

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

- all—Trace all sFlow monitoring events.
- client-server—Trace sFlow monitoring client-server events.

- configuration—Trace sFlow monitoring configuration events.
- interface—Trace sFlow monitoring interface events.
- rtsock—Trace routing socket code events.

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

no-world-readable—(Optional) Prevent any user from reading the trace file.

replace—(Optional) Replace an existing trace file if there is one.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**. Incoming trace file data is logged in the now empty **trace-file**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also specify a maximum number of trace files with the files option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 10 KB through the maximum file size of 4 GB

Default: 128 KB

world-readable—(Optional) Allow any user to read the trace file.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Overview of sFlow Technology | 970

udp-port

Syntax

```
udp-port port-number;
```

Hierarchy Level

```
[edit protocols sflow collector]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 18.1R1 for MX Series routers.
Statement introduced in Junos OS Release 18.2R1 for PTX Series routers.

Description

Configure the UDP port for a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the collector for analysis.

Options

port-number—UDP port number for this collector.

Default: 6343

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**
- Example: Configuring sFlow Technology to Monitor Network Traffic on MX Series Routers | **990**

udp-port (QFX Series)

Syntax

```
udp-port port-number;
```

Hierarchy Level

```
[edit protocols sflow collector]
```

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Configure the UDP port for a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the collector for analysis.

Default

Port 6343

Options

port-number—UDP port number for this collector.

Required Privilege Level

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

CHAPTER 63

Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options

IN THIS CHAPTER

- accounting-options | 1953
- allow-clear (Accounting Options) | 1957
- archive-sites | 1958
- class-usage-profile | 1959
- counters | 1960
- destination-classes | 1961
- fields (for Interface Profiles) | 1962
- fields (for Routing Engine Profiles) | 1964
- file (Associating with a Profile) | 1965
- file (Configuring a Log File) | 1966
- files | 1967
- filter-profile | 1968
- interface-profile | 1969
- interval (Accounting Options) | 1970
- mib-profile | 1971
- mpls (Security Forwarding Options) | 1972
- nonpersistent | 1973
- object-names | 1974
- operation | 1975
- routing-engine-profile | 1976
- size | 1977
- source-classes | 1978
- start-time (Accounting) | 1979
- traceoptions (System Accounting) | 1980
- transfer-interval | 1982

accounting-options

Syntax

```
accounting-options {
    class-usage-profile profile-name {
        file filename;
        interval minutes;
        destination-classes {
            destination-class-name;
        }
        source-classes {
            source-class-name;
        }
    }
    cleanup-interval days;
    file filename {
        archive-sites {
            site-name;
        }
        backup-on-failure (master-and-slave | master-only);
        compress;
        files number;
        nonpersistent;
        push-backup-to-master;
        size bytes;
        start-time time;
        transfer-interval minutes;
    }
    filter-profile profile-name {
        counters {
            counter-name;
        }
        file filename;
        interval minutes;
    }
    flat-file-profile profile-name{
        fields {
            all-fields;
            egress-stats {
                all-fields;
                input-bytes;
                input-packets;
                output-bytes;
                output-packets;
```

```
        queue-id;
        red-drop-bytes;
        red-drop-packets;
        tail-drop-packets;
        total-drop-packets;
    }
    general-param {
        all-fields;
        accounting-type;
        descr;
        line-id;
        logical-interface;
        nas-port-id;
        physical-interface;
        routing-instance;
        timestamp;
        user-name;
        vlan-id;
    }
    ingress-stats {
        all-fields;
        drop-packets;
        input-bytes;
        input-packets;
        output-bytes;
        output-packets;
        queue-id;
    }
    l2-stats {
        all-fields;
        input-mcast-bytes;
        input-mcast-packets;
    }
```

```
        overall-packet {
            all-fields;
            input-bytes;
            input-discards;
            input-errors;
            input-packets;
            inputv6-bytes;
            inputv6-packets;
            output-bytes;
            output-errors;
            output-packets;
            outputv6-bytes;
            outputv6-packets;
            input-v4-bytes;
            input-v4-packets;
            output-v4-bytes;
            output-v4-packets;
            input-bytes-per-sec;
            input-packets-per-sec;
        }
        service-accounting;
    }
    file filename;
    format (csv | ipdr)
    interval minutes;
    schema-version schema-name;
}
interface-profile profile-name {
    allow-clear;
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
mib-profile profile-name {
    file filename;
    interval seconds;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
```

```
    routing-engine-profile profile-name {
        fields {
            field-name;
        }
        file filename;
        interval minutes;
    }
}
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure options for accounting statistics collection.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuration Statements at the [edit accounting-options] Hierarchy Level | 844

Accounting Options Configuration | 846

allow-clear (Accounting Options)

Syntax

```
allow-clear;
```

Hierarchy Level

```
[edit accounting-options interface-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 17.3R1 on MX Series routers.

Description

Reports accounting statistics values cleared by the **clear interfaces statistics** command on a logical interface configured with accounting options to the accounting options flat file associated with the interface. By default, this statement is disabled and the cleared statistics are not reported to the flat file, although the counters do show as cleared in the CLI.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interface Profile | 864
Accounting Options Configuration | 846

archive-sites

Syntax

```
archive-sites site-name{
    password password;
}
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format ***router-name_log-filename_timestamp***. When you configure file archival by using the **archive-states** statement, the transfer file utility uses the default routing instance to connect to the destination server. If the default routing instance is unable to connect to the destination server, the transfer file utility does not work.

Starting in Junos OS Release 18.4R1, when you configure file archival by using the **archive-sites** statement, the transfer file utility does not work if you have enabled the management instance.

To delete an archive site, use the **delete** command instead of **set**.

Options

site-name—Any valid FTP/SCP/SFTP URL to a destination.

password *password*—Password for logging into the archive site.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Archive Sites for the Files | 858

class-usage-profile

Syntax

```
class-usage-profile profile-name {
    file filename;
    interval minutes;
    source-classes {
        source-class-name;
    }
    destination-classes {
        destination-class-name;
    }
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a class usage profile, which is used to log class usage statistics to a file in the **/var/log** directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has **destination-class-usage** configured.

For information about configuring source classes, see the *Junos Routing Protocols Configuration Guide*. For information about configuring source class usage, see the *Junos Network Management Configuration Guide*.

Options

profile-name—Name of the destination class profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Class Usage Profiles | 878

counters

Syntax

```
counters {
    counter-name;
}
```

Hierarchy Level

[edit accounting-options **filter-profile** *profile-name*]

Release Information

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

Description

Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the **/var/log** directory.

Options

counter-name—Name of the counter.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Counters | **868**

destination-classes

Syntax

```
destination-classes {
    destination-class-name;
}
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the destination classes for which statistics are collected.

Options

destination-class-name—Name of the destination class to include in the source class usage profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a Class Usage Profile | 878

fields (for Interface Profiles)

Syntax

```
fields {
    field-name;
}
```

Hierarchy Level

[edit accounting-options **interface-profile** *profile-name*]

Release Information

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

Description

Statistics to collect in an accounting-data log file for an interface.

Options

field-name—Name of the field:

- **input-bytes**—Input bytes
- **input-errors**—Generic input error packets
- **input-multicast**—Input packets arriving by multicast
- **input-packets**—Input packets
- **input-unicast**—Input unicast packets
- **output-bytes**—Output bytes
- **output-errors**—Generic output error packets
- **output-multicast**—Output packets sent by multicast
- **output-packets**—Output packets
- **output-unicast**—Output unicast packets
- **rpf-check-total-packets**—Total packets failing reverse-path-forwarding check
- **rpf-check-total-bytes**—Total bytes failing reverse-path-forwarding check

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interface Profile | 864

fields (for Routing Engine Profiles)

Syntax

```
fields {
    field-name;
}
```

Hierarchy Level

[edit accounting-options **routing-engine-profile** *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Statistics to collect in an accounting-data log file for a Routing Engine.

Options

field-name—Name of the field:

- **cpu-load-1**—Average system load over the last 1 minute
- **cpu-load-5**—Average system load over the last 5 minutes
- **cpu-load-15**—Average system load over the last 15 minutes
- **date**—Date, in YYYYMMDD format
- **host-name**—Hostname for the router
- **time-of-day**—Time of day, in HHMMSS format
- **uptime**—Time since last reboot, in seconds
- **cpu-usage-5sec**—System CPU usage for last 5 seconds
- **cpu-usage-1min**—Average system CPU usage for the last one minute
- **cpu-usage-5min**—Average system CPU usage for the last 5 minutes
- **free-mem**—Free memory available in MB
- **total-mem**—Total memory available in MB

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Routing Engine Profile | 884

file (Associating with a Profile)

Syntax

```
file filename;
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series Switches.

Description

Specify the accounting log file associated with the profile.

Options

filename—Name of the log file. You must specify a filename already configured in the **file** statement at the **[edit accounting-options]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interface Profile | 864
Configuring the Filter Profile | 868
Configuring the MIB Profile | 881
Configuring the Routing Engine Profile | 884

file (Configuring a Log File)

Syntax

```
file filename {
    archive-sites {
        site-name;
    }
    backup-on-failure (master-and-slave | master-only);
    compress;
    files number;
    nonpersistent;
    push-backup-to-master;
    size bytes;
    start-time time;
    transfer-interval minutes;
}
```

Hierarchy Level

[edit accounting-options]

Release Information

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

Description

Specify a log file to be used for accounting data.

Options

filename—Name of the file in which to write accounting data.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Accounting-Data Log Files | 856

Configuring Flat-File Accounting for Layer 2 Wholesale

Configuring Flat-File Accounting for Extensible Subscriber Services Management

Flat-File Accounting Overview

files

Syntax

```
files number;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Specify the maximum number of log files to be used for accounting data.

Options

number—The maximum number of files. When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for ***number*** is 3 and the default value is 10.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Accounting-Data Log Files | 856

filter-profile

Syntax

```
filter-profile profile-name {
    counters {
        counter-name;
    }
    file filename;
    interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a profile to filter and collect packet and byte count statistics and write them to a file in the **/var/log** directory. To apply the profile to a firewall filter, you include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level. For more information about firewall filters, see *Firewall Filters Overview*.

Options

profile-name—Name of the filter profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Firewall Filters Overview

Configuring the Filter Profile | 868

interface-profile

Syntax

```
interface-profile profile-name {
    allow-clear;
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a profile to filter and collect error and packet statistics and write them to a file in the **/var/log** directory. You can specify an interface profile for either a physical or a logical interface.

Options

profile-name—Name of the interface profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interface Profile | 864

Accounting Options Configuration | 846

interval (Accounting Options)

Syntax

```
interval minutes;
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **[edit accounting-options mib-profile *profile-name*]** hierarchy level added in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify how often statistics are collected for the accounting profile.

Options

minutes—Length of time between each collection of statistics.

Range: 1 through 2880 minutes

Default: 30 minutes

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Interface Profile | 864
- Configuring the Filter Profile | 868
- Configuring the MIB Profile | 881
- Configuring the Routing Engine Profile | 884

mib-profile

Syntax

```
mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Create a MIB profile to collect selected MIB statistics and write them to a file in the **/var/log** directory.

> **NOTE:** Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Options

profile-name—Name of the MIB statistics profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the MIB Profile | 881

mpls (Security Forwarding Options)

Syntax

```
mpls {
   mode packet-based;
}
```

Hierarchy Level

```
[edit security forwarding-options family]
```

Release Information

Statement introduced in Junos OS Release 9.0.

Description

Enable the forwarding of MPLS traffic. By default, the device drops MPLS traffic.

CAUTION: Because MPLS operates in packet mode, security services are not available.

NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1500, SRX5600, and SRX5800.

Required Privilege Level

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

RELATED DOCUMENTATION

- MPLS Overview

nonpersistent

Syntax

```
nonpersistent;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

Statement introduced in Junos OS Release 8.3.

Description

Store log files used for accounting data in the **mfs/var/log** directory (located on DRAM) instead of the **cf/var/log** directory (located on the compact flash drive). This feature is useful for minimizing read/write traffic on the router's compact flash drive.

> **NOTE:** If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. Therefore, you should back up these files periodically.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Storage Location of the File | 860

object-names

Syntax

```
object-names {
    mib-object-name;
}
```

Hierarchy Level

```
[edit accounting-options mib-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.

Options

mib-object-name—Name of a MIB object. You can specify more than one MIB object name.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the MIB Profile | 881

operation

Syntax

```
operation operation-name;
```

Hierarchy Level

```
[edit accounting-options mib-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the name of the operation used to collect MIB statistics for an accounting-data log file.

Options

operation-name—Name of the operation to use. You can specify a **get**, **get-next**, or **walk** operation.

Default: walk

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the MIB Profile | 881

routing-engine-profile

Syntax

```
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

Release Information

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

Description

Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the **/var/log** directory.

Options

profile-name—Name of the Routing Engine statistics profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Routing Engine Profile | 884

size

Syntax

```
size bytes;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Specify attributes of an accounting-data log file.

Options

bytes—Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.

Syntax: ***x*** to specify bytes, ***x***k to specify KB, ***x***m to specify MB, ***x***g to specify GB

Range: 256 KB through 1 GB

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Maximum Size of the File | 858

source-classes

Syntax

```
source-classes {
    source-class-name;
}
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the source classes for which statistics are collected.

Options

source-class-name—Name of the source class to include in the class usage profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a Class Usage Profile | 878

start-time (Accounting)

Syntax

```
start-time time;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the start time for transfer of an accounting-data log file.

Options

time—Start time for file transfer.

Syntax: ***YYYY-MM-DD.hh:mm***

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Start Time for File Transfer | 861

traceoptions (System Accounting)

Syntax

```
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag (all| config | events | radius | tacplus);
    no-remote-trace
}
```

Hierarchy Level

```
[edit system accounting]]
```

Release Information

Statement introduced in Junos OS Release 14.2.
tacplus option introduced in Junos OS Release 15.1.

Description

Define tracing operations for System Accounting.

Default

Trace options are not enabled by default.

Options

file *filename*—Name of the file in which Junos OS stores the accounting logs. By default, this is created under the /var/log directory.

files *number*—(Optional) Maximum number of trace files. When a trace file reaches the size specified by the size option, the filename is appended with 0 and compressed. For example, when trace file named trace-file-log reaches size <*size*>, it is renamed and compressed to trace-file-log.0.gz. When trace-file-log reaches size <*size*> or the second time, the trace-file-log.0.gz is renamed to trace-file-log.1.gz and trace-file-log is renamed and compressed to trace-file-log.0.gz. This renaming shceme ensures that the older logs to have a greater index number. When number of trace files reach <*number*> then the oldest file is deleted.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10

flag *flag*—Tracing operation to perform. You can include one or more of the following flags:

- **all**—Trace all operations.

- **config**—Trace configuration processing.
- **events**—Trace accounting events and their processing.
- **radius**—Trace RADIUS processing.
- **tacplus**—Trace TACPLUS processing.

no-remote-trace—(Optional) Disable tracing and logging operations that track normal operations, error conditions, and packets that are generated by or passed through the Juniper Networks device.

no-world-readable—Restrict access to the trace files to the owner.

Default: no-world-readable

size *size*—(Optional) Maximum size of each trace file in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). If you do not specify a unit, the default is bytes. If you specify a maximum file size, you also must specify a maximum number of trace files by using the files option and a filename by using the file option.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: size to specify bytes, sizek to specify KB, sizem to specify MB, or sizeg to specify GB.

Range: 10 KB through 1 MB

Default: 128 KB

world-readable—Enable any user to access the trace files.

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

transfer-interval

Syntax

```
transfer-interval minutes;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Options

minutes—Time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Range: 5 through 2880 minutes

Default: 30 minutes

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Transfer Interval of the File | 861

CHAPTER 64

Configuration Statements: Chassis Cluster

IN THIS CHAPTER

- cluster (Chassis) | **1984**
- global-threshold | **1987**
- global-weight | **1988**
- ip-monitoring | **1989**
- ip-monitoring (Services) | **1991**
- next-hop | **1993**

cluster (Chassis)

Syntax

```
cluster {
    configuration-synchronize (Chassis Cluster) {
        no-secondary-bootup-auto;
    }
    control-link-recovery;
    control-ports fpc {
        port;
    }
    health-monitoring;
    heartbeat-interval milliseconds;
    heartbeat-threshold heartbeat-threshold;
    network-management {
        cluster-master;
    }
    redundancy-group (Chassis Cluster) name {
        gratuitous-arp-count gratuitous-arp-count;
        hold-down-interval seconds;
        interface-monitor name {
            weight weight;
        }
        ip-monitoring {
            family {
                inet {
                    address name {
                        interface logical-interface-name {
                            secondary-ip-address;
                        }
                        weight weight;
                    }
                }
            }
            global-threshold global-threshold;
            global-weight global-weight;
            retry-count retry-count;
            retry-interval (Chassis Cluster) retry-interval;
        }
        node (Chassis Cluster Redundancy Group) (0 | 1) {
            priority priority;
        }
        preempt (Chassis Cluster) {
            delay seconds;
```

```
            limit limit;
            period seconds;
        }
    }
    redundant-interface name {
        mapping-interface mapping-interface;
    }
    reth-count (Chassis Cluster) reth-count;
    traceoptions (Chassis Cluster) {
        file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
        flag name;
        level (alert | all | critical | debug | emergency | error | info | notice | warning);
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit chassis]
```

Release Information

Statement introduced in Junos OS Release 9.0.

The **health-monitoring** option is introduced in the Junos OS Release 18.4R1.

Description

Configure a chassis cluster. Perform the configuration under the **[edit chassis cluster]** configuration stanza to define chassis cluster configuration, operations, and monitoring. This configuration must specify configuration synchronization, control link recovery, heartbeat interval and threshold, network management, redundancy group, and traceoptions.

Options

configuration-synchronize —Disable automatic chassis cluster synchronization. See *configuration-synchronize (Chassis Cluster)*.

control-link-recovery—Enable automatic control link recovery option.

control-ports—Enable specific chassis cluster control ports.

Values:

- **fpc**—FPC slot number
- **port**—Port number

health-monitoring—Enable to monitor the health status of the SRX Series devices operating in chassis cluster mode. The health status between the two nodes is monitored and shared over control links and fabric links. Failover between the nodes occurs based on the heart beat status and health status of the control links and fabric links. By default, the option is disabled.

heartbeat-interval—Interval between successive heartbeats (milliseconds)

Default: 1000

Range: 1000-2000

heartbeat-threshold—Number of consecutive missed heartbeats to indicate device failure

Default: 3

Range: 3-8

network-management—Define parameters for network management. See *network-management*.

redundancy-group *name*—Define a redundancy group. See *redundancy-group (Chassis Cluster)*.

reth-count—Number of redundant ethernet interfaces

Range: 1-128

traceoptions—Define chassis cluster redundancy process tracing operations. See *traceoptions (Chassis Cluster)*.

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

ip-monitoring | **1989**

global-threshold

Syntax

```
global-threshold number;
```

Hierarchy Level

```
[edit chassis cluster redundancy-group group-number ip-monitoring ]
```

Release Information

Statement introduced in Junos OS Release 10.1.

Description

Define global threshold for IP monitoring. This is the number that needs to be met or exceeded by all of the cumulative weights of the monitored IP addresses to trigger a failover.

When a monitored address is marked as unreachable, the weight value associated with that address is deducted from the the redundancy group IP address monitoring global threshold. If the accumulated monitored address weight values surpass the global-threshold value, that is, when the global threshold reaches 0, the global weight is deducted from the redundancy group threshold. Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered

Options

number—Value at which the IP monitoring weight is applied against the redundancy group failover threshold.

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

ip-monitoring | 1989

global-weight

Syntax

```
global-weight number;
```

Hierarchy Level

```
[edit chassis cluster redundancy-group group-number ip-monitoring]
```

Release Information

Statement introduced in Junos OS Release 10.1.

Description

Define global weight for IP monitoring. This is the weight that is subtracted from the redundancy group weight for all of the hosts being monitored. This number specifies the relative importance of IP address monitored objects in the operation of the redundancy group.

Every monitored IP address is assigned a weight. If the monitored address becomes unreachable, the weight of the object is deducted from the global-threshold of IP monitoring objects in its redundancy group. When the global-threshold reaches 0, the global-weight is deducted from the redundancy group. Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.

Options

number —Combined weight assigned to all monitored IP addresses. A higher weight value indicates a greater importance.

Range: 0 through 255

Default: 255

Required Privilege Level

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

RELATED DOCUMENTATION

ip-monitoring | 1989

ip-monitoring

Syntax

```
ip-monitoring {
    family {
        inet {
            ipv4-address {
                interface {
                    logical-interface-name;
                    secondary-ip-address ip-address;
                }
                weight number;
            }
        }
    }
    global-threshold number;
    global-weight number;
    retry-count number;
    retry-interval seconds;
}
```

Hierarchy Level

[edit **chassis cluster redundancy-group *group-number***]

Release Information

Statement updated in Junos OS Release 10.1.

Description

Specify a global IP address monitoring threshold and weight, and the interval between pings (**retry-interval**) and the number of consecutive ping failures (**retry-count**) permitted before an IP address is considered unreachable for all IP addresses monitored by the redundancy group. Also specify IP addresses, a monitoring weight, a redundant Ethernet interface number, and a secondary IP monitoring ping source for each IP address, for the redundancy group to monitor.

Options

IPv4 address—The address to be continually monitored for reachability. You also set up a secondary IP address to allow testing from the secondary node.

NOTE: All monitored object failures, including IP monitoring, are deducted from the redundancy group threshold priority. Other monitored objects include interface monitor, SPU monitor, cold-sync monitor, and NPC monitor (on supported platforms).

interface *interface* secondary-ip-address *ip-address*;—Define source address for monitoring packets on secondary link.

global-threshold—Define global threshold for IP monitoring. See **global-threshold**.

Default: 0

Range: 0-255

global-weight—Define global weight for IP monitoring. See **global-weight**.

Default: 255

Range: 0-255

retry-count—Number of retries needed to declare reachablity failure. See *retry-count (Chassis Cluster)*.

Default: 5

Range: 5-15

retry-interval—Define the time interval in seconds between retries. See *retry-interval (Chassis Cluster)*.

Default: 1

Range: 1-30

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

Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring | **966**

ip-monitoring (Services)

Syntax

```
ip-monitoring {
    policy policy-name {
        match {
            rpm-probe [probe-name];
        }
        no-preempt ;
        then {
            interface interface-name (disable | enable);
            preferred-route {
                withdraw;
                route destination-address {
                    discard
                    next hop next-hop;
                    preferred-metric metric;
                    }
                routing-instances name;
            }
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Support added for the **discard** option starting from Junos OS Release 15.1X49-D60.

Support added for the **withdraw** option starting from Junos OS Release 20.3R1.

Description

Configure IP monitoring.

Options

withdraw—Remove the primary routes when RPM fails to probe the destination. So, the traffic can choose other routes in the route table. If no other route exists, then the traffic is dropped. When you run the **show services ip-monitoring status** command, in the output, the status of the route **WITHDRAWED** indicates that this route is removed. See **show services ip-monitoring status** for more details.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

icmp | **2007**

next-hop

Syntax

```
next-hop next-hop;
```

Hierarchy Level

```
[edit services rpm probe owner test test-name]
```

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Specify the next-hop address to which the probe should be sent.

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

RELATED DOCUMENTATION

probe | 1726

CHAPTER 65

Configuration Statements: Datapath Debug

IN THIS CHAPTER

- action-profile | **1995**
- capture-file (Security) | **1997**
- datapath-debug | **1999**
- flow (Security Flow) | **2001**
- icmp | **2007**
- maximum-capture-size (Datapath Debug) | **2008**
- traceoptions (Security Datapath Debug) | **2009**

action-profile

Syntax

```
action-profile profile-name {
    event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress | pot) {
        count;
        packet-dump;
        packet-summary;
        trace;
    }
    module {
        flow {
            flag {
                all;
            }
        }
    }
    preserve-trace-order;
    record-pic-history;
}
```

Hierarchy Level

```
[edit security datapath-debug]
```

Release Information

Command introduced in Junos OS Release 10.0.

Description

Configure the action profile options for data path debugging.

Options

- ***action-profile name*** — Name of the action profile.
- **event**—Enable the events to trace the packet when the packet hit the events (jexec, lbt, lt-enter, lt-leave, mac-egress, mac-ingress, np-egress, np-ingress, pot)
  - **count**—Number of times a packet hits the specified event.
  - **packet-dump**—Capture the packet that hits the specified event.
  - **packet-summary**—Print the source/destination IP address details with protocol number and IP length details along with trace message for the specified event.
  - **trace**—Print the standard trace message when the packet hits the specified event.

- **module**—Turn on the flow session related trace messages.
  - **flow**—Trace flow session related messages.
  - **flag**—Specify which flow message needs to be traced.
  - **all**—Trace all possible flow trace messages.
  - **trace**—Print the standard trace message when the packet hits the specified event.
- **preserve-trace-order**—Preserve trace order.
- **record-pic-history**—Record the PICs in which the packet has been processed.

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

RELATED DOCUMENTATION

Example: Configuring Packet Capture for Datapath Debugging | 1672

capture-file (Security)

Syntax

```
capture-file {
    filename;
    files number;
    format pacp-format;
    size maximum-file-size;
    (world-readable | no-world-readable);
}
```

Hierarchy Level

```
[edit security datapath-debug]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Sets packet capture for performing the datapath-debug action.

Options

- ***filename***—Name of the file to receive the output of the packet capturing operation.
- **files**—Maximum number of capture files.

  If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

  Range: 1 through 10 files
- **format**—Describes the format of the capture file. The default format file is pcap. You can also set it as private (binary) format.
- **size**—Describes the size limit of the capture file.

  If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

  Range: 10 KB through 100 MB
- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

Required Privilege Level

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

RELATED DOCUMENTATION

- System Log Messages

datapath-debug

Syntax

```
datapath-debug {
    action-profile name {
        event name {
            count;
            packet-dump;
            packet-summary;
            trace;
        }
        module name {
            flag name;
        }
        preserve-trace-order;
        record-pic-history;
    }
    capture-file (Security) filename <files files> <format pcap> <size size> <(world-readable | no-world-readable)>;
    maximum-capture-size (Datapath Debug) bytes;
    packet-filter name {
        action-profile (default | profile);
        destination-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec |
            finger | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate |
            kshell | ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd
            | nntp | ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap | snpp
            | socks | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt |
            zephyr-hm | zephyr-srv);
        destination-prefix destination-prefix;
        interface interface;
        protocol (ah | egp | esp | gre | icmp | icmp6 | igmp | ipip | number | ospf | pim | rsvp | sctp | tcp | udp);
        source-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec | finger
            | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate | kshell |
            ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd | nntp |
            ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap | snpp | socks
            | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt | zephyr-hm |
            zephyr-srv);
        source-prefix source-prefix;
    }
    traceoptions (Security Datapath Debug) {
        file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
        no-remote-trace;
    }
}
```

Hierarchy Level

[edit security]

Release Information

Command introduced in Junos OS Release 10.0.

Description

Configure the data path debugging options.

> **NOTE:** Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Understanding Data Path Debugging for Logical Systems*

flow (Security Flow)

Syntax

```
flow {
    advanced-options {
        drop-matching-link-local-address;
        drop-matching-reserved-ip-address;
        reverse-route-packet-mode-vr;
    }
    aging {
        early-ageout seconds;
        high-watermark percent;
        low-watermark percent;
    }
    allow-dns-reply;
    allow-embedded-icmp;
    allow-reverse-ecmp;
    enable-reroute-uniform-link-check {
        nat;
    }
    enhanced-routing-mode;
    ethernet-switching {
        block-non-ip-all;
        bpdu-vlan-flooding;
        bypass-non-ip-unicast;
        no-packet-flooding {
            no-trace-route;
        }
    }
    force-ip-reassembly;
    ipsec-performance-acceleration (Security Flow);
    load-distribution {
        session-affinity {
            ipsec;
        }
    }
    mcast-buffer-enhance;
    multicast-nh-resolve-retry multicast-nh-resolve-retry-value;
    packet-log (Security Flow) {
        enable;
        packet-filter name {
            conn-tag conn-tag;
            destination-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec
                | finger | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate |
```

```
            kshell | ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd
            | nntp | ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap |
            snpp | socks | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt
            | zephyr-hm | zephyr-srv);
        destination-prefix destination-prefix;
        interface interface;
        logical-system logical-system;
        protocol (ah | egp | esp | gre | icmp | icmp6 | igmp | ipip | number | ospf | pim | rsvp | sctp | tcp | udp);
        source-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec |
            finger | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate |
            kshell | ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd
            | nntp | ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap |
            snpp | socks | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt
            | zephyr-hm | zephyr-srv);
        source-prefix source-prefix;
    }
    throttle-interval milliseconds;
}
pending-sess-queue-length (high | moderate | normal);
power-mode-ipsec;
preserve-incoming-fragment-size;
route-change-timeout seconds;
strict-packet-order;
syn-flood-protection-mode (syn-cookie | syn-proxy);
sync-icmp-session;
tcp-mss (Security Flow) {
    all-tcp {
        mss mss;
    }
    gre-in {
        mss mss;
    }
    gre-out {
        mss mss;
    }
    ipsec-vpn (Security Flow) {
        mss mss;
    }
}
```

```
tcp-session {
    fin-invalidate-session;
    maximum-window (128K | 1M | 256K | 512K | 64K);
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    strict-syn-check;
    tcp-initial-timeout seconds;
    time-wait-state {
        (session-ageout | session-timeout seconds);
        apply-to-half-close-state;
    }
}
traceoptions (Security Flow) {
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
    flag name;
    no-remote-trace;
    packet-filter name {
        conn-tag conn-tag;
        destination-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec
            | finger | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate |
            kshell | ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd
            | nntp | ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap |
            snpp | socks | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt
            | zephyr-hm | zephyr-srv);
        destination-prefix destination-prefix;
        interface interface;
        logical-system logical-system;
        protocol (ah | egp | esp | gre | icmp | icmp6 | igmp | ipip | number | ospf | pim | rsvp | sctp | tcp | udp);
        source-port (afs | bgp | biff | bootpc | bootps | cmd | cvspserver | dhcp | domain | eklogin | ekshell | exec |
            finger | ftp | ftp-data | http | https | ident | imap | kerberos-sec | klogin | kpasswd | krb-prop | krbupdate |
            kshell | ldap | ldp | login | mobileip-agent | mobilip-mn | msdp | netbios-dgm | netbios-ns | netbios-ssn | nfsd
            | nntp | ntalk | ntp | pop3 | pptp | printer | radacct | radius | range | rip | rkinit | smtp | snmp | snmptrap |
            snpp | socks | ssh | sunrpc | syslog | tacacs | tacacs-ds | talk | telnet | tftp | timed | who | xdmcp | zephyr-clt
            | zephyr-hm | zephyr-srv);
        source-prefix source-prefix;
    }
    rate-limit rate-limit;
    trace-level {
        (brief | detail | error);
    }
}
```

```
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement modified in Junos OS Release 9.5. The **power-mode-ipsec** option added in Junos OS Release 18.3R1 for vSRX instances, in Junos OS Release 18.4R1 for SRX4100 and SRX4200 devices, and in Junos OS Release 18.2R2 for SRX5400, SRX5600, and SRX5800 devices. The **multicast-nh-resolve-retry** and the **strict-packet-order** options are added in Junos OS Release 20.2R2 for SRX345 and SRX1500 devices.

Description

Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

Options

advanced-options— Flow configuration advanced options.

Values:

- drop-matching-link-local-address—Drop matching link local address.
- drop-matching-reserved-ip-address—Drop matching reserved source IP address.
- reverse-route-packet-mode-vr—Allow reverse route lookup with packet mode vr.

allow-dns-reply— Allow unmatched incoming DNS reply packet.

allow-embedded-icmp— Allow embedded ICMP packets not matching a session to pass through.

allow-reverse-ecmp— Allow reverse ECMP route lookup.

enable-reroute-uniform-link-check— Enable reroute check with uniform link.

Values:

- nat—Enable NAT check.

enhanced-routing-mode— Enable enhanced route scaling.

force-ip-reassembly— Force to reassemble IP fragments.

ipsec-performance-acceleration— Accelerate the IPSec traffic performance.

mcast-buffer-enhance— Allow to hold more packets during multicast session creation.

multicast-nh-resolve-retry—You can use this command configure the multicast route next-hop resolve attempts. When a multicast route next-hop resolve is unsuccessful, the SRX Series device attempts to resolve the next-hop route based on the specified retry counts.

Default: 0

Range: 0 through 20

pending-sess-queue-length— Maximum queued length per pending session.

Values:

- high—Maximum number of queued sessions.
- moderate—Allow more queued sessions than normal.
- normal—Normal number of sessions queued.

power-mode-ipsec— Enable power mode ipsec processing.

preserve-incoming-fragment-size— Preserve incoming fragment size for egress MTU.

route-change-timeout— Timeout value for route change to nonexistent route (seconds).

Default: 6

Range: 6 through 1800

strict-packet-order—You can use this command to maintain multicast traffic order and resolve packet drop issue.

syn-flood-protection-mode— TCP SYN flood protection mode.

Values:

- syn-cookie—Enable SYN cookie protection.
- syn-proxy—Enable SYN proxy protection.

sync-icmp-session—Allow icmp sessions to sync to peer node.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Understanding Traffic Processing on Security Devices*
- *Understanding Session Characteristics for SRX Series Services Gateways*
- *Understanding Packet Flow in Logical Systems for SRX Series Devices*

icmp

Syntax

```
icmp{
    destination-interface interface-name;
}
```

Hierarchy Level

```
[edit services rpm probe-server]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the port information for the ICMP server.

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

- Understanding ICMP Fragment Protection

maximum-capture-size (Datapath Debug)

Syntax

```
maximum-capture-size maximum-capture-size;
```

Hierarchy Level

```
[edit security datapath-debug]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Specifies maximum packet capture length.

Options

- **maximum-capture-size *maximum-capture-size***—Specify the maximum packet capture length.

Range: 68 through 10,000 bytes

Required Privilege Level

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

RELATED DOCUMENTATION

System Log Messages

traceoptions (Security Datapath Debug)

Syntax

```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    no-remote-trace;
}
```

Hierarchy Level

```
[edit security datapath-debug]
```

Release Information

Command introduced in Junos OS Release 9.6.

Description

Sets the trace options for datapath-debug.

> **NOTE:** Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

Options

- **file**—Configure the trace file 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, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

    Range: 2 through 1000 files

Default: 10 files

- **match *regular-expression***—Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed trace-file.0. When 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 a filename.

  Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

  Range: 10 KB through 1 GB

  Default: 128 KB
- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option

- **no-remote-trace**—Set remote tracing as disabled.

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

CHAPTER 66

Configuration Statements: Health Monitoring

IN THIS CHAPTER

- falling-threshold | **2012**
- health-monitor | **2013**
- health-monitor (KHMS) | **2014**
- idp (SNMP) | **2016**
- routing-engine (SNMP Resource Level) | **2017**
- interval (Health Monitor) | **2019**
- rising-threshold | **2020**

falling-threshold

Syntax

```
falling-threshold percentage;
```

Hierarchy Level

```
[edit snmp health-monitor],
[edit snmp health-monitor idp]
```

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.3 for the **[edit snmp health-monitor idp]** hierarchy level.

Description

Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

percentage—The lower threshold for the alarm entry.

Range: **1** through **100**

Default: **70** percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold or Rising Threshold | **836**

rising-threshold | **2020**

health-monitor

Syntax

```
health-monitor {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
    idp {
        falling-threshold percentage;
        interval seconds;
        rising-threshold percentage;
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option **idp** introduced in Junos OS Release 9.3 for all supported platforms.

Description

Configure health monitoring.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Health Monitoring on Devices Running Junos OS | 834

health-monitor (KHMS)

Syntax

```
health-monitor {
    ifstate-clients {
        (peer-stuck | non-peer-stuck | all-clients-stuck);
    }
    threshold-level {
        (low | medium | high);
    }
    action {
        (alarm | alarm-with-cores | restart);
    }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 16.1R1.

Description

Configure the kernel health monitoring system (KHMS). The KHMS is used to detect and take action on stuck ifstate clients. Stuck ifstate clients can affect system performance. With this configuration statement you can configure a time interval in which the system can detect a stuck ifstate client. You also can configure the action the system takes when it finds a stuck ifstate client.

The ifstate clients receive states from the kernel. There are two kinds of ifstate clients:

- non-peer clients (for example, some daemons, or processes, on the Routing Engine)—ifstate non-peer clients open connections between programs and read states from or write states to the kernel.
- peer clients (for example, FPCs)—ifstate peer clients read peer messages and send updates to the peers.

An ifstate client is stuck if the kernel sends a message and the ifstate client does not send back an ACK. A rt_pfe_veto condition is a log message that indicates that states are sent but no ACK comes back. However, the system won't take the configured action until the configured time interval times outs, in case the ACK comes late.

Options

ifstate-clients—Configure which ifstate clients you want to monitor and manage. There are three options:

- **peer-stuck**—Monitor and manage stuck peers.
- **non-peer-stuck**—Monitor and manage stuck processes.
- **all-clients-stuck**—Monitor and manage both stuck peers and stuck processes.

threshold-level—Configure the time interval in which to detect if a given ifstate client is stuck:

- **high**—540 seconds
- **medium**—360 seconds; this is the default.
- **low**—180 seconds

action—Configure the action to be taken on the stuck ifstate client once the configured time interval times out.

- **alarm**—Only an alarm will be raised about the stuck ifstate client; this is the default.
- **alarm-with-cores**—An alarm will be raised about the stuck ifstate client after collecting live cores from the master Routing Engine kernel and the stuck peer.

CAUTION: In the case of a stuck peer, collecting lives cores might result in the component being restarted or rebooted.

- **restart**—The stuck ifstate client will be disconnected after collecting live cores from the master Routing Engine kernel and the stuck peer (depending on supportability).

CAUTION: When choosing this action, be aware of the implications of restarting an ifstate client. For example, some FPCs don't simply restart; they reboot.

Required Privilege Level
admin

idp (SNMP)

Syntax

```
idp {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
}
```

Hierarchy Level

```
[edit snmp health-monitor]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Configure health monitoring for Intrusion Detection and Prevention (IDP).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Health Monitoring on Devices Running Junos OS | 834

routing-engine (SNMP Resource Level)

Syntax

```
routing-engine {
   resource <cpu | memory | open-files-count | process-count | storage | temperature | traceoptions > ;
   {
      interval <interval in secs>;
      moderate-threshold <percentage level>;
      high-threshold <percentage level>;
      critical-threshold <percentage level>;
      action <monitor | prevent | recover>;
   }
}
```

Hierarchy Level

```
[edit snmp health-monitor routing-engine]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10. Statement modified in Junos OS Release 15.1X49-D10.

Description

Override the global configuration for a resource.

Options

- **interval**—Monitoring interval in seconds.

  Range: 1 through 604800 seconds

  Default: 300 seconds

- **moderate-threshold**—Percentage of moderate threshold level resource utilization.

  Range: 30 through 99 percent

  Default: 70 percent

- **high-threshold** —Percentage of high-threshold level resource utilization.

  Range: 30 through 99 percent

  Default: 80 percent

- **critical-threshold** —Percentage of critical threshold level resource utilization.

  Range: 30 through 99 percent

Default: 90 percent

- **action**–Enable action for all resources.

  Default: If action is not enabled, the default action is prevent.

WARNING: If the system health management action for an affected resource is configured to recover, then certain instrusive operations necessary for preventing system breakdown are taken. Instrusive operations can include restarting or terminating processes, deleting files, and so on. Such action information is logged in the system health management history and system log.

Required Privilege Level

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

interval (Health Monitor)

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp health-monitor],
[edit snmp health-monitor idp]
```

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.3 for the **[edit snmp health-monitor idp]** hierarchy level.

Description

Interval between samples.

Options

seconds—Time between samples, in seconds.

Range: **1** through **2147483647** seconds

Default: **300** seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interval | **837**

rising-threshold

Syntax

```
rising-threshold percentage;
```

Hierarchy Level

```
[edit snmp health-monitor],
[edit snmp health-monitor idp]
```

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.3 for the **[edit snmp health-monitor idp]** hierarchy level.

Description

Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

percentage—The lower threshold for the alarm entry.

Range: **1** through **100**

Default: **80** percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

falling-threshold | **2012**

Configuring the Falling Threshold or Rising Threshold | **836**

CHAPTER 67

Configuration Statements: Remote Monitoring (RMON)

IN THIS CHAPTER

- alarm (SNMP RMON) | **2022**
- community | **2023**
- description | **2024**
- event | **2025**
- falling-event-index | **2026**
- falling-threshold | **2027**
- falling-threshold-interval | **2028**
- interval | **2029**
- request-type | **2030**
- rising-event-index | **2031**
- rising-threshold | **2032**
- rmon | **2033**
- sample-type | **2034**
- startup-alarm | **2035**
- syslog-subtag | **2036**
- type | **2037**
- variable | **2038**

alarm (SNMP RMON)

Syntax

```
alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    request-type (get-next-request | get-request | walk-request);
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
    syslog-subtag syslog-subtag;
    variable oid-variable;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure RMON alarm entries.

Options

index—Identifies this alarm entry as an integer.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Alarm Entry and Its Attributes | 784

event | 2025

RMON MIB Event, Alarm, Log, and History Control Tables | 781

Monitoring RMON MIB Tables | 642

Understanding RMON | 774

community

Syntax

```
community community-name;
```

Hierarchy Level

```
[edit snmp rmon event index]
```

Release Information

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

Description

The trap group that is used when generating a trap (if **eventType** is configured to send traps). If that trap group has the **rmon-alarm** trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of **eventCommunity**). If nothing is configured, traps are sent to each group with the **rmon-alarm** category set.

Options

community-name—Identifies the trap group that is used when generating a trap if the event is configured to send traps.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

description

Syntax

```
description description;
```

Hierarchy Level

```
[edit snmp rmon alarm index],
[edit snmp rmon event index]
```

Release Information

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

Description

Text description of alarm or event.

Options

description—Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Description | 785
Configuring an RMON Event Entry and Its Attributes | 789

event

Syntax

```
event index {
    community community-name;
    description description;
    type type;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

Release Information

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

Description

Configure RMON event entries.

Options

index—Identifier for a specific event entry.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

alarm (SNMP RMON) | 2022

falling-event-index

Syntax

```
falling-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

The index of the event entry that is used when a falling threshold is crossed. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a falling threshold is crossed.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Event Index or Rising Event Index | 785

rising-event-index | 2031

falling-threshold

Syntax

```
falling-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Set the lower threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—The lower threshold for the alarm entry.

Range: -2,147,483,648 through 2,147,483,647

Default: 20 percent less than **rising-threshold**

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold or Rising Threshold | 786

rising-threshold | 2032

falling-threshold-interval

Syntax

```
falling-threshold-interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Set the interval between samples after the rising threshold is exceeded and the value of the sample starts to drop. If the value of the sample drops and exceeds the falling threshold, the regular sampling interval is used.

Options

seconds—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold Interval | 787

interval | 2029

interval

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Interval between samples.

Options

seconds—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interval | 786

request-type

Syntax

```
request-type (get-next-request | get-request | walk-request);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Extend monitoring to a specific SNMP object instance (**get-request**), or extend monitoring to all object instances belonging to a MIB branch (**walk-request**), or extend monitoring to the next object instance after the instance specified in the configuration (**get-next-request**).

Options

get-next-request—Performs an SNMP get next request.

get-request—Performs an SNMP get request.

walk-request—Performs an SNMP walk request.

Default: walk-request

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Request Type | 787

variable | 2038

rising-event-index

Syntax

```
rising-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Index of the event entry that is used when a rising threshold is crossed. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a rising threshold is crossed.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Event Index or Rising Event Index | 785

falling-event-index | 2026

rising-threshold

Syntax

```
rising-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Set the upper threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—The lower threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold or Rising Threshold | 786

falling-threshold | 2027

rmon

Syntax

```
rmon { ... }
```

Hierarchy Level

```
[edit snmp]
```

Release Information

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

Description

Configure Remote Monitoring.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Alarm Entry and Its Attributes | 784

sample-type

Syntax

```
sample-type (absolute-value | delta-value);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Method of sampling the selected variable.

Options

absolute-value—Actual value of the selected variable is used when comparing against the thresholds.

delta-value—Difference between samples of the selected variable is used when comparing against the thresholds.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Sample Type | 787

startup-alarm

Syntax

```
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

The alarm that can be sent upon entry startup.

Options

falling-alarm—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.

rising-alarm—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.

rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

Default: rising-or-falling-alarm

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Startup Alarm | 788

syslog-subtag

Syntax

```
syslog-subtag syslog-subtag;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Add a tag to the system log message.

Options

syslog-subtag *syslog-subtag*—Tag of not more than 80 uppercase characters to be added to syslog messages.

Default: None

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the System Log Tag | 788

type

Syntax

```
type type;
```

Hierarchy Level

```
[edit snmp rmon event index]
```

Release Information

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

Description

Type of notification generated when a threshold is crossed.

Options

type—Type of notification:

- **log**—Add an entry to **logTable**.
- **log-and-trap**—Send an SNMP trap and make a log entry.
- **none**—No notifications are sent.
- **snmptrap**—Send an SNMP trap.

Default: log-and-trap

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

variable

Syntax

variable *oid-variable*;

Hierarchy Level

[edit snmp rmon **alarm** *index*]

Release Information

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

Description

Object identifier (OID) of MIB variable to be monitored.

Options

oid-variable—OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, **1.3.6.1.2.1.2.1.2.2.1.10.1**). Alternatively, use the MIB object name (for example, **ifInOctets.1**).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Variable | 789

CHAPTER 68

Configuration Statements: Resource Monitoring for Memory Regions

IN THIS CHAPTER

- free-fw-memory-watermark (Resource Monitor) | **2040**
- free-heap-memory-watermark (Resource Monitor) | **2041**
- free-nh-memory-watermark (Resource Monitor) | **2042**
- high-cos-queue-threshold | **2043**
- high-threshold (Resource Monitor) | **2044**
- no-load-throttle (Resource Monitor) | **2045**
- no-logging (Resource Monitor) | **2046**
- no-throttle (Resource Monitor) | **2047**
- resource-category jtree (Resource Monitor) | **2048**
- resource-type (Resource Monitor) | **2050**
- subscribers-limit (Resource Monitor) | **2052**
- traceoptions (Resource Monitor) | **2054**

free-fw-memory-watermark (Resource Monitor)

Syntax

```
free-fw-memory-watermark number;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Configure the percentage of free memory space used for firewall or filters to be monitored with a watermark value. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

Options

number—Percentage of free memory space used for firewall and filters to be monitored with a watermark value. When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.

Range: 1 through 100

Required Privilege Level

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

free-heap-memory-watermark (Resource Monitor)

Syntax

```
free-heap-memory-watermark number;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Configure the percentage of free memory space used for ukernel or heap (ASIC) memory to be monitored with a watermark value. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

Options

number—Percentage of free memory space used for ukernel or heap to be monitored with a watermark value. When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.

Range: 1 through 100

Required Privilege Level

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

free-nh-memory-watermark (Resource Monitor)

Syntax

```
free-nh-memory-watermark number;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Configure the percentage of free memory space used for next-hops to be monitored with a watermark value. The default value and the configured value of the watermark value for the percentage of free next-hop memory also applies to encapsulation memory. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

Options

number—Percentage of free memory space used for next-hops to be monitored with a watermark value. The NH memory watermark is applicable only for encapsulation memory (output WAN static RAM memory). When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.

Range: 1 through 100

Required Privilege Level

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

high-cos-queue-threshold

Syntax

```
high-cos-queue-threshold number;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 17.4R1.

Description

Configure the class-of-service (CoS) queue threshold by percentage.

> **NOTE:** This feature is only available when you enable subscriber management. For more information on enabling subscriber management, see *Configuring Junos OS Enhanced Subscriber Management*.

This CoS resource monitoring feature bases admission decisions only on queues. Other CoS resources are not part of this criteria. This feature does not support throttling for subscribers arriving on pseudo-wire, logical tunnel, or redundant logical tunnel devices. The feature is supported on the following hardware:

- MX240, MX480, and MX960 routers
- MPC2E legacy, MPC2E-NG, MPC3E-NG, MPC5E, and MPC7E line cards

Options

number—High-threshold percentage for CoS queue utilization per scheduler. When CoS queue utilization on a given FPC reaches that FPC's configured threshold level, further subscriber logins on that FPC are not allowed. This resource monitoring mechanism provides adjustable safety margins to proactively avoid completely exhausting each FPC's available CoS queue resources. Starting in Junos OS Release 19.4R1, you can specify a value of 0, which means that no subscribers are throttled based on CoS queue throttling.

Range: 0 through 90

Default: 100

Required Privilege Level

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

RELATED DOCUMENTATION

Resource Monitoring for Subscriber Management and Services Overview

high-threshold (Resource Monitor)

Syntax

```
high-threshold number;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Configure the high threshold value, exceeding which warnings or error logs are generated, for all the regions of memory, such as heap or ukernel, next-hop and encapsulation, and firewall filter memory. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

Options

number—High threshold percentage for memory resource utilization

Range: 1 through 100

Required Privilege Level

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

no-load-throttle (Resource Monitor)

Syntax

```
no-load-throttle;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information
Statement introduced in Junos OS Release 17.3R1 for MX series routers.

Description
The no-load-throttle statement disables line card load-based throttling. Load-based throttling is also disabled when you configure the no-throttle statement.

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

no-logging (Resource Monitor)

Syntax

```
no-logging;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Disable the generation of error log messages when the utilization of memory resources exceeds the threshold or checkpoint levels. By default, messages are written to /var/log/rsmonlog.

Options

no-logging—Disable the generation of error log messages when the utilization of memory resources exceeds the configured level. By default, error logs are recorded when the resource level utilization is exceeded.

Required Privilege Level

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

no-throttle (Resource Monitor)

Syntax

```
no-throttle;
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Disable the throttling of subscriber services and sessions when the utilization of memory resources exceeds the threshold levels. For the subscriber service management, sessions are throttled based on line card resources, such as heap, counter memory, expansion memory, and firewall counter memory. If the resource has been used above a certain threshold, the subscribers and services are throttled to prevent the system from being overloaded and resulting in a breakdown. This feature gathers input from each of the line cards and transfers this statistical detail to the Routing Engine process using a well-known internal port. This information is scanned by the daemon on the Routine Engine and using the shared memory space built into the the session database, the existing active subscribers and sessions are throttled. You can configure the resource-monitoring capability on MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

Options

no-throttle—Disable the throttling of subscriber services and sessions when the utilization of memory resources exceeds the threshold levels. The throttling capability is enabled by default.

Required Privilege Level

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

resource-category jtree (Resource Monitor)

Syntax

```
resource-category jtree {
resource-type (contiguous-pages | free-dwords | free-pages) {
    low-watermark number;
    high-watermark number;
}
}
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Define the resource category that you want to monitor and analyze for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. The resource category includes detailed CPU utilization, session rate, and session count statistics. You use the resource category statistics to understand the extent to which new attack objects or applications affect performance. The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. The Junos OS provides the memory-enhanced statement to reallocate the jtree memory for routes, firewall filters, and Layer 3 VPNs.

Options

jtree—Specify the Jtree resource category for which you want to monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Diagnosing and Debugging System Performance by Configuring Memory Resource Usage Monitoring on MX Series Routers | **1619**

resource-type (Resource Monitor)

Syntax

```
resource-type (contiguous-pages | free-dwords | free-pages) {
    low-watermark number;
    high-watermark number;
}
```

Hierarchy Level

```
[edit system services resource-monitor resource-category jtree]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Configure the type of resource for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. You can monitor the memory utilization of resource types on MX Series routers with DPCs and MPCs.

Options

continguous-pages | free-dwords | free-pages—Select one of the following options:

- **contiguous-pages**—Specify that memory resource utilization needs to be monitored for contiguous memory blocks or pages.
- **free-dwords**—Specify that memory resource utilization needs to be monitored for free or unused memory double words (dwords).
- **free-pages**—Specify that memory resource utilization needs to be monitored for free or unused memory blocks or pages.

low-watermark *number*—Configure the lower range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the low threshold value is exceeded, error log messages are generated.

Range: 1 through 100

high-watermark *number*—Configure the higher range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the high threshold value is exceeded, error log messages are generated.

Range: 1 through 100

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Diagnosing and Debugging System Performance by Configuring Memory Resource Usage Monitoring on MX Series Routers | **1619**

subscribers-limit (Resource Monitor)

Syntax

```
subscribers-limit {
    client-type (any | dhcp | l2tp | pppoe) {
        chassis {
            limit limit;
        }
        fpc slot-number {
            limit limit;
            pic number {
                limit limit;
                port number {
                    limit limit;
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 17.3R1.

Description

Configure the maximum number of subscribers of a specified client type allowed to be logged in on the chassis, per MPC, per MIC, and per port. When that number is reached, subsequent logins are denied until the current number of subscribers drops below the maximum allowed.

Limit the number of subscribers allowed to log in per chassis, MPC, MIC, or port.

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

Limiting Subscribers by Client Type and Hardware Element with Resource Monitor

Resource Monitoring for Subscriber Management and Services

traceoptions (Resource Monitor)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag;
}
```

Hierarchy Level

```
[edit system services resource-monitor]
```

Release Information

Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

Description

Define tracing operations for the memory resource utilization processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. All files are placed in the directory **/var/log**.

Default: rmopd

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

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

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.

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

no-world-readable—(Default) Disable unrestricted file access. This means the log file can be accessed only by the user who configured the tracing operation.

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.

Required Privilege Level

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

CHAPTER 69

Configuration Statements: Security Alarms

IN THIS CHAPTER

- decryption-failures | **2057**
- idp (Security Alarms) | **2058**

decryption-failures

Syntax

```
decryption-failures {
    threshold value;
}
```

Hierarchy Level

```
[edit security alarms potential-violation]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Raise a security alarm after exceeding a specified number of decryption failures.

Default

Multiple decryption failures do not cause an alarm to be raised.

Options

failures—Number of decryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

Range: 1 through 1,000,000,000.

Default: 1000

Required Privilege Level

security—To view this statement in the configuration.

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

RELATED DOCUMENTATION

IPsec VPN Overview

Monitoring VPN Traffic

idp (Security Alarms)

Syntax

```
idp;
```

Hierarchy Level

```
[edit security alarms potential-violation]
```

Release Information
Statement introduced in Junos OS Release 11.2.

Description
Configure alarms for IDP attack.

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

CHAPTER 70

Configuration Statements: Network Analytics

IN THIS CHAPTER

- address (Analytics Collector) | **2060**
- agent (Analytics) | **2062**
- analytics | **2065**
- collector (Analytics) | **2072**
- depth-threshold | **2074**
- export-profiles | **2076**
- file (Analytics) | **2079**
- inputs (Analytics) | **2081**
- interface (Export Profiles) | **2086**
- interfaces (Analytics Resource) | **2088**
- interfaces (Analytics) | **2090**
- latency-threshold | **2092**
- local (Analytics Collector) | **2094**
- outputs (Analytics) | **2095**
- queue-statistics | **2099**
- resource (Analytics) | **2101**
- resource-profiles (Analytics) | **2103**
- service-agents (Analytics) | **2105**
- streaming-servers | **2107**
- system (Analytics Resource) | **2109**
- system (Export Profiles) | **2111**
- traceoptions (Analytics) | **2113**
- traceoptions (Analytics Agent) | **2114**
- traffic-statistics | **2116**

address (Analytics Collector)

Syntax

```
address ip-address {
    port number {
        transport protocol {
            export-profile profile-name;
        }
    }
}
```

Hierarchy Level

```
[edit services analytics collector]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure the address of a remote server to receive streamed analytics (queue and traffic statistics) data.

NOTE: The **address** statement is not available in Junos OS Releases prior to 13.2X51-D15.

Options

ip-address—IP address of the remote server receiving the streamed data.

port *number*—Port number of the remote server receiving the streaming data.

export-profile *profile-name*—Name of the export profile containing the parameters for the analytics data being streamed.

transport *protocol*—A transport protocol used to stream data to the port.

Values:

- **tcp**—Transmission Control Procol (TCP)
- **udp**—User Datagram Protocol (UDP)

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Network Analytics Overview | 1120

agent (Analytics)

Syntax

```
agent {
  service-agents {
    agent-name {
      inputs {
        analytics {
          parameters {
            generate-tags value;
            sample-frequency value;
            sensors file-path;
          }
        }
        input-ipfix {
          parameters {
            maximum-connections number;
            tcp-port port-number;
            vrf-name name;
          }
        }
        input-jti-ipfix {
          parameters {
            record-group group-name {
              record ipfix-record-name;
              reporting-interval seconds;
            }
          }
        }
      }
      outputs {
        file {
          parameters {
            path file-path;
          }
        }
        kafka {
          parameters {
            server ip-address;
            topic topic-name;
            encoding encoding-type;
          }
        }
        output-ipfix {
```

```
            parameters {
              collector-address ip-address;
              collector-ca-certificate file-path;
              collector-certificate file-path;
              collector-certificate-key file-path;
              collector-connection-retry-interval seconds;
              collector-tcp-port port-number;
              collector-vrf-name vrf-name;
            }
          }
        }
      }
    }
    traceoptions {
      filename filename;
      flag (debug | error | info | trace);
    }
}
```

Hierarchy Level

```
[edit services analytics]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.

Description

Configure the Network Telemetry Framework (NTF) agent and corresponding service agents that use input and output plug-ins to collect, transform, and forward network telemetry data.

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

RELATED DOCUMENTATION

- *Configuring the BNG as an IPFIX Mediator to Collect and Export IPFIX Data*
- *Configuring the Collection and Export of Local Telemetry Data on the IPFIX Mediator*
- *Configuring NTF Agent*
- *IPFIX Mediation on the BNG*
- *Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector*

analytics

List of Syntax

Syntax (EX Series and QFX Series) on page 2065
Syntax (MX Series & PTX Series) on page 2069

Syntax (EX Series and QFX Series)

Junos OS Release 13.2X51-D15 and later:

```
analytics {
    collector {
        local {
            file filename {
                size size;
                files number;
            }
        }
        address ip-address {
            port number {
                transport protocol {
                    export-profile profile-name;
                }
            }
        }
    }
    export-profiles {
        profile-name {
            interface {
                information;
                statistics {
                    queue;
                    traffic;
                }
                status {
                    link;
                    queue;
                    traffic;
                }
            }
            stream-format format;
            system {
                information;
                status {
                    queue;
```

```
                traffic;
            }
        }
    }
}
resource {
    interfaces {
        interface-name {
            resource-profile name;
        }
    }
    system {
        polling-interval {
            queue-monitoring interval;
            traffic-monitoring interval;
        }
        resource-profile name;
    }
}
resource-profiles {
    profile-name {
        depth-threshold {
            high number;
            low number;
        }
        latency-threshold {
            high number;
            low number;
        }
        no-queue-monitoring;
        no-traffic-monitoring;
        queue-monitoring;
        traffic-monitoring;
    }
}
traceoptions {
    file filename {
        files number;
        size size;
    }
}
}
```

Junos OS Release 13.2X50-D15 and 13.2X51-D10 only:

```
analytics {
    interfaces {
        all {
            depth-threshold high number low number;
            latency-threshold high number low number;
            queue-statistics;
            no-queue-statistics;
            traffic-statistics;
            no-traffic-statistics;
        }
        interface-name {
            depth-threshold high number low number;
            latency-threshold high number low number;
            queue-statistics;
            no-queue-statistics;
            traffic-statistics;
            no-traffic-statistics;
        }
    }
    queue-statistics {
        file filename {
            files number-of-files;
            size size;
        }
        interval interval;
    }
    streaming-servers {
        address ip-address {
            port number {
                stream-format format;
                stream-type type
            }
        }
    }
    traceoptions {
        file filename {
            files number;
            size size;
        }
    }
    traffic-statistics {
        file filename {
            files number-of-files;
```

```
            size size;
        }
        interval interval;
    }
}
```

Syntax (MX Series & PTX Series)

```
analytics {
  agent {
    service-agents {
      agent-name {
        inputs {
          analytics {
            parameters {
              generate-tags value;
              sample-frequency value;
              sensors file-path;
            }
          }
          input-ipfix {
            parameters {
              maximum-connections number;
              tcp-port port-number;
              vrf-name name;
            }
          }
          input-jti-ipfix {
            parameters {
              record-group group-name {
                record ipfix-record-name;
                reporting-interval seconds;
              }
            }
          }
        }
        outputs {
          file {
            parameters {
              path file-path;
            }
          }
          kafka {
            parameters {
              server ip-address;
              topic topic-name;
              encoding encoding-type;
            }
          }
          output-ipfix {
            parameters {
```

```
                collector-address ip-address;
                collector-ca-certificate file-path;
                collector-certificate file-path;
                collector-certificate-key file-path;
                collector-connection-retry-interval seconds;
                collector-tcp-port port-number;
                collector-vrf-name vrf-name;
            }
        }
    }
  }
  traceoptions {
    filename filename;
    flag (debug | error | info | trace);
  }
 }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 13.2 on QFX Series switches.
Statement introduced in Junos OS Release 13.2X51-D25 on EX Series switches.
Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.

Description

Configure the network analytics feature that includes monitoring for traffic and queue statistics. The network analytics processes running on the Packet Forwarding Engine and Routing Engine collect and analyze the data, and generate reports that may be saved in log files or sent as streaming data to remote servers.

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

Network Analytics Overview | **1120**

Configuring the BNG as an IPFIX Mediator to Collect and Export IPFIX Data

Configuring NTF Agent

IPFIX Mediation on the BNG

Configuring the Collection and Export of Local Telemetry Data on the IPFIX Mediator

Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector

collector (Analytics)

Syntax

```
collector {
    local {
        file filename {
            size size;
            files number;
        }
    }
    address ip-address {
        port number {
            transport protocol {
                export-profile profile-name;
            }
        }
    }
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure a local file for storing network analytics statistics and/or a remote server for receiving streamed statistics data.

NOTE: The **collector** statement is not available in Junos OS Releases prior to 13.2X51-D15.

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

Network Analytics Overview | 1120

depth-threshold

Syntax

```
depth-threshold {
    high number;
    low number;
}
```

Hierarchy Level

```
[edit services analytics interfaces]
[edit services analytics resource-profiles]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement in the **[edit services analytics resource-profiles]** hierarchy level introduced in Junos OS Release 13.2X51-D15.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

If network analytics queue statistics monitoring is enabled, specify the high and low values (in bytes) of the queue depth (buffer) threshold. If you configure a depth threshold, you cannot configure the latency threshold. You can configure the depth threshold for one interface or all interfaces. Specify the high and low queue depth threshold numbers:

> **NOTE:** The configuration for a specific interface supersedes the global configuration for all interfaces.

Options

high *number*—Specify the maximum value for the depth threshold.

Range: 1 to 1,250,000,000 bytes

Default:

- Junos OS Release 13.2X51-D10 or later—0 bytes
- Junos OS Release 13.2X50-D15—14,680,064 bytes (14 MB)

low *number*—Specify the minimum value for the depth threshold.

Range: 1 to 1,250,000,000 bytes

Default:

- Junos OS Release 13.2X51-D10 or later—0 bytes
- Junos OS Release 13.2X50-D15—1024 bytes (1 KB)

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**
latency-threshold | **2092**
resource-profiles (Analytics) | **2103**

export-profiles

Syntax

```
export-profiles {
   profile-name {
      interface {
         information;
         statistics {
            queue;
            traffic;
         }
         status {
            link;
            queue;
            traffic;
         }
      }
      stream-format format;
      system {
         information;
         status {
            queue;
            traffic;
         }
      }
   }
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure an profile to specify the network analytics data being streamed to remote servers. Each profile is a template that defines the type of data being streamed.

> **NOTE:** The **export-profile** statement is not available in Junos OS Releases prior to 13.2X51-D15.

Options

profile-name—Name of the export profile containing the configuration of the data being streamed.

stream-format *format*—Format of the streaming data being sent to a server. Only one format can be sent to each port on a server.

Values:

- **csv**—Comma-separated Values (CSV). Data sent in this format is newline separated, and each record contains one stream type (queue or traffic data) per interface.Each record contains either a “q” for a queue statistics, or a “t” for a traffic statistics.
- **gpb**—Google Protocol Buffer (GPB). Data sent in this format has a hierachical format, and is categorized by resource type (system or interfaces), which is specified in the message header. You can generate data formatted in other formats (CSV, TSV, and JSON) from GPB-encoded data.

  Each message includes a 8-byte header containing the following information:

  - Bytes 0 to 3—Length of the message.
  - Byte 4—Message version.
  - Bytes 5 to 7—Reserved for future use.

  > **NOTE:** A schema file called **analytics.proto** containing the definitions of the GPB messages is available for downloading from the following location:
  >
  > https://www.juniper.net/documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt

- **json**—JavaScript Object Notation (JSON). Data sent in this format is newline separated, and each record contains one stream type (queue or traffic data) per interface. Each record contains either “queue-statistics” or “traffic-statistics” in the “record type” field.
- **tsv**—Tab-separated Values (TSV). Data sent in this format is newline separated, and each record contains one stream type (queue or traffic data) per interface. Each record contains a “q” for a queue statistics, or a “t” for a traffic statistics.

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

Network Analytics Overview | 1120

file (Analytics)

Syntax

```
file filename {
    files number-of-files;
    size size;
}
```

Hierarchy Level

```
[edit services analytics collector local]
[edit services analytics queue-statistics]
[edit services analytics traffic-statistics]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Enable the logging of queue or traffic monitoring statistics in a local file. This statement does not enable monitoring.

Default

This feature is disabled by default.

Options

filename—Specify a filename for storing queue and traffic monitoring statistics in the Comma-separated Values (CSV) format. The file is stored in the **/var/log/** directory of your device.

If you do not specify a filename, the data is not stored in a file.

NOTE: In Junos OS Release 13.2X51-D15 or later, you configure a single filename to store both queue and traffic monitoring statistics. In Junos OS Release 13.2X51-D10 and earlier, you configure separate files for storing monitoring data, one for queue statistics, and another for traffic statistics.

files *number-of-files*—Specify the number of files to store locally. After the number of files with the maximum file size is reached, the system starts over and writes the data to the first file.

Range: 2 to 1,000 files.

size *size*—Configure the file size in megabytes (MB).

Syntax: ***xm*** to specify MB.

Range: 10 to 4095 MB

Required Privilege Level

interface—To view this statement in the configuration.

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

Release History Table

Release	Description
13.2X51-D15	In Junos OS Release 13.2X51-D15 or later, you configure a single filename to store both queue and traffic monitoring statistics.
13.2X51-D10	In Junos OS Release 13.2X51-D10 and earlier, you configure separate files for storing monitoring data, one for queue statistics, and another for traffic statistics.

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

inputs (Analytics)

Syntax

```
inputs {
    analytics {
        parameters {
            generate-tags value;
            sample-frequency value;
            sensors path;
        }
    }
    input-ipfix {
        parameters {
            maximum-connections number;
            tcp-port port-number;
            vrf-name name;
        }
    }
    input-jti-ipfix {
        parameters {
            record-group group-name {
                record ipfix-record-name;
                reporting-interval seconds;
            }
        }
    }
}
```

Hierarchy Level

[edit services analytics agent **service-agents** *agent-name*]

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.
input-jti-ipfix option added in Junos OS Release 18.4R1 on MX Series routers.
analytics option added in Junos OS Release 18.4R1 on MX Series and PTX Series routers.

Description

Configure parameters for a Network Telemetry Framework (NTF) service agent input plug-in. For each service agent instance, you can configure more than one input plug-in to push data to the output plug-in.

NOTE: When you modify the input plug-in configuration of a service agent instance, the associated service agent daemon is restarted.

Options

analytics parameters—Configure parameters to collect data from Junos Telemetry Interface (JTI) sensors.

generate-tags *value*—(Optional) Enable tag generation.

Default: Enabled

sample-frequency *value*—Specify the frequency interval (in seconds) at which the JTI sensor generates data to export to the data collector. Range is from 0 to 24 hours.

Default: 5 seconds

sensors *file-path*—Specify the resource string associated with the JTI sensor for collecting JTI data from a specific resource. The format is a file path and must be entered exactly. For a list of available JTI resource string options, see the *sensor* configuration statement and *Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface)* documentation.

input-ipfix parameters—Configure parameters for the IPFIX mediation service agent to gather and consolidate IPFIX records from downstream devices.

NOTE: Any change you make to an existing **input-ipfix** plug-in configuration restarts the IPFIX service agent daemon to apply the changes.

NOTE: Although each of the parameters has a default value, you must configure at least one of the parameters to enable the plug-in. If you configure only one parameter and want to use the default value, you must specify that value.

maximum-connections *number*—(Optional) Maximum number of TCP connections that the IPFIX mediator can support.

Range: 1 through 500

Default: 100

tcp-port *port-number*—(Optional) TCP port on the IPFIX mediator that receives TCP packets; the listening port.

Default: 4739

vrf-name *name*—(Optional) Name of the VRF (routing instance) in which IPFIX packets are accepted.

Default: default

input-jti-ipfix parameters—Configure parameters for the IPFIX mediation service agent to collect and report local sensor data from the BNG configured as an IPFIX mediator. For each group of records, the plug-in subscribes to the specific sensor data sets associated with each record.

When you remove a record group from the configuration, the sensor sets for the member records are unsubscribed. The template IDs for the associated IPFIX records are returned to the pool for re-use.

record *ipfix-record-name*—One of the following individual IPFIX records associated with a nonconfigurable set of local sensor data. See *Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector* for the sensors collected by each record.

address-pool-utilization	port-statistics
chassis-inventory	resource-utilization
chassis-power	subscriber-statistics
dhcpv4-server-stats	thermal
interface-metadata	uptime
interface-queue-statistics	

BEST PRACTICE: We recommend that you configure the **interface-metadata** record whenever you configure the **interface-queue-statistics** record. The metadata information is essential for understanding details about the subscriber whose queue statistics are being collected.

record-group *group-name*—Name of a group of IPFIX records that subscribes to the sensor data sets associated with the individual records that comprise the record group. You can configure a maximum of 10 record groups.

reporting-interval *seconds*—(Optional) Interval in seconds between reports for the subscribed sensor data. The interval applies to all records (and all sensor sets) in the record group.

Range: 60 through 86,400 seconds

Default: 900 seconds

Required Privilege Level

system

RELATED DOCUMENTATION

- *Configuring the BNG as an IPFIX Mediator to Collect and Export IPFIX Data*
- *Configuring the Collection and Export of Local Telemetry Data on the IPFIX Mediator*
- *Configuring NTF Agent*
- *IPFIX Mediation on the BNG*
- *Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector*

interface (Export Profiles)

Syntax

```
interface {
    information;
    statistics {
        queue;
        traffic;
    }
    status {
        link;
        queue;
        traffic;
    }
}
```

Hierarchy Level

```
[edit services analytics export-profiles]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure an export profile for streaming network analytics data for a specific interface to remote servers. Each profile is a template that defines the type of data being streamed for that interface.

> **NOTE:** The **interface** statement is not available in Junos OS Releases prior to 13.2X51-D15.

Options

information—Information about the specified interface, including SNMP index, interface index, slot, port number, media type, capability, and port type.

statistics—Type of monitoring statistics to be streamed.

Values:

- **queue**
- **traffic**

status—Status information about the interface to be streamed.

Values:

- **link**
- **queue**
- **traffic**

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

interfaces (Analytics Resource)

Syntax

```
interfaces {
    interface-name {
        resource-profile profile-name;
    }
}
```

Hierarchy Level

```
[edit services analytics resource]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Apply the network analytics resource profile to an interface for which you wish to enable queue or traffic statistics monitoring. The resource profile is a template that specifies the parameters for queue and traffic monitoring, as well as for the depth and latency thresholds.

> **NOTE:** The **interfaces** statement in the **[edit services analytics resource]** hierarchy is not available in Junos OS Releases prior to 13.2X51-D15.

Options

interface-name—Name of the interface for which a resource profile has been configured.

resource-profile *profile-name*—Name of a resource profile containing the analytics parameters that have been specified for interfaces. Information contained in a resource profile includes the configuration of queue and traffic monitoring (whether enabled or disabled), and values for the depth and latency thresholds (if applicable).

Required Privilege Level

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

RELATED DOCUMENTATION

interfaces (Analytics)

Syntax

```
interfaces {
    all {
        depth-threshold high number low number;
        latency-threshold high number low number;
        queue-statistics;
        no-queue-statistics;
        traffic-statistics;
        no-traffic-statistics;
    }
    interface-name {
        depth-threshold high number low number;
        latency-threshold high number low number;
        queue-statistics;
        no-queue-statistics;
        traffic-statistics;
        no-traffic-statistics;
    }
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure physical interfaces for monitoring traffic and queue statistics by the network analytics processes running on the Packet Forwarding Engine and Routing Engine. You may specify one interface or all interfaces in your configuration.

NOTE: The configuration for a specific interface supersedes the global configuration for all interfaces. You can configure traffic and queue monitoring for physical interfaces only; logical interfaces and Virtual Chassis port (VCP) interfaces are not supported.

> **NOTE:** Disabling the queue or traffic monitoring (using the **no-queue-statistics** or **no-traffic-statistics** configuration statements) supersedes the configuration (enabling) of the feature.

Options

all—Configure all interfaces on the device for high-frequency monitoring.

interface-name—Name of the interface to configure for high-frequency monitoring.

no-queue-statistics—Disable the collection of queue statistics.

> **NOTE:** The **no-queue-statistics** statement supersedes the **queue-statistics** statement.

no-traffic-statistics—Disable the collection of traffic statistics.

> **NOTE:** The **no-traffic-statistics** statement supersedes the **traffic-statistics** statement.

queue-statistics—Enable the collection of queue statistics for a specific interface or all interfaces.

traffic-statistics—Enable the collection of traffic statistics for a specific interface or all 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

Network Analytics Overview | 1120

latency-threshold

Syntax

```
latency-threshold {
    high number;
    low number;
}
```

Hierarchy Level

```
[edit services analytics interfaces]
[edit services analytics resource-profiles]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement in the **[edit services analytics resource-profiles]** hierarchy level introduced in Junos OS Release 13.2X51-D15.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

If network analytics queue statistics monitoring is enabled, specify the high and low values (in microseconds) of the latency threshold of the queue. If you configure a latency threshold, you cannot configure the depth threshold. You can configure the latency threshold for one interface or all interfaces. Specify the high and low latency threshold numbers:

> **NOTE:** The configuration for a specific interface supersedes the global configuration for all interfaces.

Options

high *number*—Specify the maximum value for the latency threshold.

Range:

- Junos OS Release 13.2X51-D15 or later—1 to 100,000,000 nanoseconds (0.001 to 100,000 microseconds)
- Junos OS Release 13.2X51-D10 or earlier—1 to 100,000 microseconds

Default:

- Junos OS Release 13.2X51-D15 or later—1,000,000 nanoseconds (1000 microseconds or 1 millisecond)

- Junos OS Release 13.2X51-D10—1000 microseconds
- Junos OS Release 13.2X50-D15—900 microseconds

low *number*—Specify the minimum value for the latency threshold.

Range:

- Junos OS Release 13.2X51-D15 or later—1 to 100,000,000 nanoseconds
- Junos OS Release 13.2X51-D10 or earlier—1 to 100,000 microseconds

Default:

- Junos OS Release 13.2X51-D15 or later—100 nanoseconds (0.1 microseconds)
- Junos OS Release 13.2X51-D10—50 microseconds
- Junos OS Release 13.2X50-D15—300 microseconds

Required Privilege Level

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**
depth-threshold | **2074**

local (Analytics Collector)

Syntax

```
local {
    file filename {
        size size;
        files number;
    }
}
```

Hierarchy Level

```
[edit services analytics collector]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure a local file for logging network analytics (queue and traffic) statistics.

> **NOTE:** The **local** statement is not available in Junos OS Releases prior to 13.2X51-D15.

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

Network Analytics Overview | 1120
collector (Analytics) | 2072

outputs (Analytics)

Syntax

```
outputs {
    file {
        parameters {
            path file-path;
        }
    }
    kafka {
        parameters {
            server ip-address;
            topic topic-name;
            encoding encoding-type;
        }
    }
    output-ipfix {
        parameters {
            collector-address ip-address;
            collector-ca-certificate file-path;
            collector-certificate file-path;
            collector-certificate-key file-path;
            collector-connection-retry-interval seconds;
            collector-tcp-port port-number;
            collector-vrf-name vrf-name;
        }
    }
}
```

Hierarchy Level

[edit services analytics agent **service-agents** *agent-name*]

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.
kafka and **file** options added in Junos OS Release 18.4R1 on MX Series and PTX Series routers.

Description

Configure parameters for the Network Telemetry Framework (NTF) agent output plug-in.

NOTE: When you modify the output plug-in configuration of a service agent instance, the associated service agent daemon is restarted.

Options

file parameters—Configure parameters for sending data in a log file to a data collector.

path *pathname*—Path for the log file to which to save the data. For example, **path /tmp/example_file.log**

kafka parameters—Configure parameters for sending data to a Kafka data collector.

server *ip-address*—IP address of the Kafka server.

topic *filename*—Kafka topic name. The naming convention of the topic is *server-name*.jti.*encoding-type*. The encoding type options are **avro**, **json**, or **msgpack**.

encoding *encoding-type*—Encoding type. Options are **avro**, **json**, or **msgpack**.

output-ipfix parameters—Configure parameters for the IPFIX mediation service agent to send the IPFIX records that have been consolidated on the router to the IPFIX collector.

You must configure the IP address of the upstream IPFIX collector. When you optionally configure at least one of the collector certificate options (**collector-ca-certificate**, **collector-certificate**, and **collector-certificate-key**), the IPFIX mediator attempts to use TLS to connect with the collector. Otherwise, the mediator uses a TCP connection.

NOTE: Any change you make to an existing **output-ipfix** output plug-in configuration restarts the IPFIX service agent daemon to apply the changes.

collector-address *ip-address*—IP address of the upstream IPFIX collector.

collector-ca-certificate *file-path*—(Optional) Path for the certificate, provided by a trusted certificate authority (CA), that is used to sign the peer certificate at the peer (IPFIX collector) level. The certificate is expected to be in .pem container format.

collector-certificate *file-path*—(Optional) Path for the client certificate that the server (IPFIX collector) uses to authenticate the client and enable mutual authentication. The fully-qualified domain name (FQDN) of both the client and the server are stored in the certificate's Subject Alternative Name field when the client and server certificates are generated. The certificate is expected to be in .pem container format.

collector-certificate-key *file-path*—(Optional) Private key file that is loaded to decrypt the encrypted message sent from the peer.

collector-connection-retry-interval *seconds*—(Optional) Interval in seconds at which the output plug-in retries connecting to the IPFIX collector.

Range: 1 through 25

Default: 20

collector-tcp-port *port-number*—(Optional) Number of the TCP port used to connect to the IPFIX collector.

Default: 4740

collector-vrf-name *vrf-name*—(Optional) Name of the VRF (routing instance) in which IPFIX packets are routed.

Default: default

Required Privilege Level

system

RELATED DOCUMENTATION

- *Configuring the BNG as an IPFIX Mediator to Collect and Export IPFIX Data*
- *Configuring the Collection and Export of Local Telemetry Data on the IPFIX Mediator*
- *Configuring NTF Agent*
- *IPFIX Mediation on the BNG*
- *Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector*

queue-statistics

Syntax

```
queue-statistics {
    file filename {
        files number-of-files;
        size size;
    }
    interval interval;
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Enable the logging of queue statistics in a local file. This statement does not enable queue statistics monitoring.

To enable queue monitoring, you must specify the **queue-statistics** configuration statement at the **[edit services analytics interfaces]** hierarchy level.

Default

This feature is disabled by default.

Options

interval *interval*—Configure the polling interval in milliseconds.

NOTE: You can configure the polling interval for queue statistics globally for all interfaces only. Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.

Range:

- Junos OS Release 13.2X50-D15—8 to 1000 milliseconds (8 milliseconds to 1 second)
- Junos OS Release 13.2X51-D10 or later—10 to 1000 milliseconds (10 milliseconds to 1 second)

NOTE: In Junos OS Release 13.2X51-D10 or later, if you configured an interval of less than 10 milliseconds, the following warning messages appear during the commit process: **Queue statistics polling interval can not be less than 10 milliseconds** and **Setting Queue statistics polling interval to 10 milliseconds**. These messages do not stop the commit operation, but the interval is automatically set to 10 milliseconds.

Default:

- Junos OS Release 13.2X50-D15—8 milliseconds
- Junos OS Release 13.2X51-D10 or later—10 milliseconds

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

Network Analytics Overview | 1120

resource (Analytics)

Syntax

```
resource {
    interfaces {
        interface-name {
            resource-profile profile-name;
        }
    }
    system {
        polling-interval {
            queue-monitoring interval;
            traffic-monitoring interval;
        }
        resource-profile profile-name;
    }
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure network analytics resources such as resource profiles (for interfaces and system), and polling intervals (for queue and traffic monitoring).

NOTE: The **resource** statement is not available in Junos OS Releases prior to 13.2X51-D15.

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

resource-profiles (Analytics)

Syntax

```
resource-profiles {
    profile-name {
        depth-threshold {
            high number;
            low number;
        }
        latency-threshold {
            high number;
            low number;
        }
        no-queue-monitoring;
        no-traffic-monitoring;
        queue-monitoring;
        traffic-monitoring;
    }
}
```

Hierarchy Level

```
[edit services analytics]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure resource profiles that are used as templates for specifying network analytics parameters. You use resource profiles to enable and disable queue and traffic monitoring, and specify depth and latency thresholds as applicable. Once you have defined a resource profile, you can apply it specifically to individual interfaces, or globally to a system.

NOTE: The **resource-profiles** statement is not available in Junos OS Releases prior to 13.2X51-D15.

The remaining statements are explained separately. See CLI Explorer.

Options

profile-name—Specify a name for the resource profile.

no-queue-monitoring—Disable queue monitoring.

no-traffic-monitoring—Disable traffic monitoring.

queue-monitoring—Enable queue monitoring.

traffic-monitoring—Enable traffic monitoring.

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

service-agents (Analytics)

Syntax

```
service-agents {
    agent-name {
        inputs {
            analytics {
                parameters {
                    generate-tags value;
                    sample-frequency value;
                    sensors file-path;
                }
            }
            input-ipfix {
                parameters {
                    maximum-connections number;
                    tcp-port port-number;
                    vrf-name name;
                }
            }
            input-jti-ipfix {
                parameters {
                    record-group group-name {
                        record ipfix-record-name;
                        reporting-interval seconds;
                    }
                }
            }
        }
        outputs {
            file {
                parameters {
                    path file-path;
                }
            }
            kafka {
                parameters {
                    server ip-address;
                    topic topic-name;
                    encoding encoding-type;
                }
            }
            output-ipfix {
                parameters {
```

```
            collector-address ip-address;
            collector-ca-certificate file-path;
            collector-certificate file-path;
            collector-certificate-key file-path;
            collector-connection-retry-interval seconds;
            collector-tcp-port port-number;
            collector-vrf-name vrf-name;
        }
    }
  }
 }
}
```

Hierarchy Level

[edit services analytics **agent**]

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.

Description

Configure a network analytics service agent that uses input and output plug-ins to collect, transform, and forward network telemetry data.

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

RELATED DOCUMENTATION

- *Configuring the BNG as an IPFIX Mediator to Collect and Export IPFIX Data*
- *Configuring the Collection and Export of Local Telemetry Data on the IPFIX Mediator*
- *Configuring NTF Agent*
- *IPFIX Mediation on the BNG*
- *Telemetry Data Collection on the IPFIX Mediator for Export to an IPFIX Collector*

streaming-servers

Syntax

```
streaming-servers {
    address ip-address {
        port number {
            stream-format format;
            stream-type type
        }
    }
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure remote servers to receive streaming output for the network analytics monitoring of traffic and queue statistics. The streaming function supports TCP connections only, and sends records separated by a newline character.

> **NOTE:** Before you use the remote server to receive streaming data, you must set up the TCP server software to process records that are separated by the newline character (\n).

You can configure multiple servers and multiple ports on each server to receive the streaming data. You can configure different streaming data types and formats for different ports on a server, but you can configure only one streaming type and one format for each port on a server.

Options

address *ip-address*—IP address of the remote server receiving the streaming data.

port *number*—Port number of the remote server receiving the streaming data.

stream-format *format*—Format of the streaming data being sent to a server. Only one format can be sent to each port on a server.

Values:

- **csv**—Comma-separated Values (CSV). Records sent in this format contain a “q” for a queue statistics, or a “t” for a traffic statistics.
- **json**—JavaScript Object Notification (JSON). Records sent in this format contain “queue-statistics” or “traffic-statistics” in the “record type” field.
- **tsv**—Tab-separated Values (TSV). Records sent in this format contain a “q” for a queue statistics, or a “t” for a traffic statistics.

stream-type *type*—Type of streaming data sent to a port. You can specify different types of streaming data to be sent to different ports on the same server.

Values:

- **queue-statistics**
- **traffic-statistics**

Required Privilege Level

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

Understanding Network Analytics Streaming Data | **1140**

system (Analytics Resource)

Syntax

```
system {
    polling-interval {
        queue-monitoring interval;
        traffic-monitoring interval;
    }
    resource-profile profile-name;
}
```

Hierarchy Level

```
[edit services analytics resource]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Apply a network analytics resource profile to a system for which you wish to enable queue or traffic monitoring. The resource profile is a template that specifies the parameters for queue and traffic monitoring, as well as for the depth and latency thresholds.

> **NOTE:** The **system** statement in the **[edit services analytics resource]** hierarchy is not available in Junos OS Releases prior to 13.2X51-D15.

Options

polling-interval—Configure the polling interval for queue and traffic monitoring:

- **queue-monitoring *polling-interval***—Configure the queue monitoring interval in milliseconds.

  Range: 1 to 1000 milliseconds (1 millisecond to 1 second) on devices other than EX4300 switches.8 to 1000 milliseconds (8 milliseconds to 1 second) on EX4300 switches.

- **traffic-monitoring *polling-interval***—Configure the traffic monitoring interval in seconds.

  Range: 1 to 300 seconds (1 second to 5 minutes) on devices other than EX4300 switches.5 to 300 seconds (5 seconds to 5 minutes) on EX 4300 switches.

resource-profile *profile-name*—Name of a resource profile containing the global analytics parameters that have been configured for the system. Information contained in a resource profile includes the

configuration of queue and traffic monitoring (whether enabled or disabled), and values for the depth and latency thresholds (if applicable).

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Network Analytics Overview | 1120

system (Export Profiles)

Syntax

```
system {
    information;
    status {
        queue;
        traffic;
    }
}
```

Hierarchy Level

```
[edit services analytics export-profiles]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure a system-wide export profile for streaming network analytics data to remote servers. Each profile is a template that defines the type of data being streamed for that system.

> **NOTE:** The **system** statement is not available in Junos OS Releases prior to 13.2X51-D15.

Options

information—Information about the system, including boot time, model, serial number, maximum number of ports, collector information, and interface list.

status—System status information to be streamed.

Values:

- **queue**
- **traffic**

Required Privilege Level

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

RELATED DOCUMENTATION

Network Analytics Overview | 1120

traceoptions (Analytics)

Syntax

```
traceoptions {
    file filename;
    files number-of-files;
    size size;
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 on QFX Series switches.
Statement introduced in Junos OS Release 13.2X51-D25 on EX Series switches.

Description

Configure traceoptions for the network analytics daemon (analyticsd) running on the Routing Engine.

Options

file *filename*—Specify a filename for storing the traceoptions data. The file is stored in the **/var/log/** directory of your device.

If you do not specify a filename, the data is not stored in a file.

files *number-of-files*—Specify the number of files to store locally. After the number files witsh the maximum file size is reached, the system starts over and writes the data to the first file.

Range: 2 to 1,000 files.

size *size*—Configure the file size in megabytes (MB).

Syntax: ***xm*** to specify MB.

Range: 10 to 4095 MB

Required Privilege Level

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

RELATED DOCUMENTATION

Network Analytics Overview | 1120

traceoptions (Analytics Agent)

Syntax

```
traceoptions {
    file filename;
    flag (debug | error | info | trace);
}
```

Hierarchy Level

[edit services analytics agent]

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series routers.
Statement introduced in Junos OS Release 18.4R1 on PTX Series routers.

Description

Configure tracing operations for Network Telemetry Framework (NTF) agent. You can specify the name of the file where the NTF agent log messages are stored. You can also specify a severity level for messages to be logged. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **trace**. As levels become more restrictive, fewer messages are logged.

> **NOTE:** Although the syntax uses the keyword **flag**, its function in this statement corresponds to the **level** keyword used for other **traceoptions** statements.

Options

file *filename*—Name of the file to receive the output of the tracing operation. The file is stored in the **/var/log/** directory of your device.

Default: ntf-agent

flag (debug | error | info | trace)—Specify the severity level for messages to be logged. The order of severity, from most to least severe is as follows:

error > info > debug > trace

- **debug**—Match debug messages.
- **error**—Match error messages. This is the most restrictive level.
- **info**—Match informational messages.

- **trace**—Match all messages.

Default: error

Required Privilege Level
system

RELATED DOCUMENTATION

> *IPFIX Mediation on the BNG*
>
> *Configuring NTF Agent*

traffic-statistics

Syntax

```
traffic-statistics {
    file filename {
        files number-of-files;
        size size;
    }
    interval interval;
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Enable the logging of traffic statistics in a local file. This statement does not enable traffic statistics monitoring.

To enable the monitoring of traffic statistics, configure the **traffic-statistics** configuration statement at the **[edit services analytics interfaces]** hierarchy level.

Default

This feature is disabled by default.

Options

file *filename*—Specify a filename for storing the traffic statistics in the JavaScript Object Notification (JSON) format. The file is stored in the **/var/log/** directory of your device.

If you do not specify a filename, the data is not stored in a file.

files *number-of-files*—Specify the number of files to store locally. After the number files with the maximum file size is reached, the system starts over and writes the data to the first file.

Range: 2 to 1,000 files.

interval *interval*—Configure the polling interval in seconds.

NOTE: You can configure the polling interval for traffic statistics globally for all interfaces only. Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.

Range:

- Junos OS Release 13.2X51-D10 or later—2 to 300 seconds (2 seconds to 5 minutes)
- Junos OS Release 13.2X50-D15—1 to 300 seconds (1 second to 5 minutes)

NOTE: In Junos OS Release 13.2X51-D10 or later, if you configured an interval of less than 2 seconds, the following warning messages appear during the commit process:

Traffic statistics polling interval can not be less than 2 seconds, and

Setting Traffic statistics polling interval to 2 seconds.

These messages do not stop the commit operation, but the interval is automatically set to 2 seconds.

Default:

- Junos OS Release 13.2X50-D15—1 second
- Junos OS Release 13.2X51-D10 or later—2 seconds

size *size*—Configure the file size in megabytes (MB).

Syntax: ***xm*** to specify MB.

Range: 10 to 4095 MB

Required Privilege Level

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

RELATED DOCUMENTATION

Network Analytics Overview | **1120**

CHAPTER 71

Configuration Statements: SNMP

IN THIS CHAPTER

- access (SNMP) | **2122**
- access-list | **2123**
- address (SNMP) | **2124**
- address-mask | **2125**
- agent-address | **2126**
- alarm-id | **2127**
- alarm (SNMP RMON) | **2128**
- alarm-list-name | **2130**
- alarm-management | **2131**
- alarm-state | **2133**
- authentication-md5 | **2135**
- authentication-none | **2136**
- authentication-password | **2137**
- authentication-sha | **2138**
- authorization | **2139**
- authorization | **2140**
- bucket-size | **2141**
- categories | **2142**
- client-list | **2144**
- client-list-name | **2145**
- clients | **2146**
- commit-delay | **2147**
- community (SNMP) | **2148**
- community | **2150**
- community (RMON) | **2151**
- community-name | **2152**
- contact (SNMP) | **2153**
- customization (SNMP) | **2154**

- description | **2155**
- description | **2156**
- description (RMON) | **2157**
- destination-port | **2158**
- engine-id | **2159**
- enterprise-oid | **2161**
- event | **2162**
- event | **2163**
- falling-event-index | **2164**
- falling-event-index (RMON) | **2165**
- falling-threshold (Health Monitor) | **2166**
- falling-threshold (RMON) | **2167**
- falling-threshold | **2168**
- falling-threshold-interval | **2169**
- falling-threshold-interval | **2170**
- filter-duplicates | **2171**
- filter-interfaces | **2172**
- group (Defining Access Privileges for an SNMPv3 Group) | **2173**
- group (Configuring Group Name) | **2174**
- health-monitor | **2175**
- history | **2176**
- interface (SNMP) | **2177**
- interface (SNMP RMON History) | **2178**
- interval | **2179**
- interval (Health Monitor) | **2180**
- interval (SNMP RMON) | **2181**
- local-engine | **2182**
- location (SNMP) | **2183**
- logical-system | **2184**
- logical-system-trap-filter | **2185**
- message-processing-model | **2186**
- name | **2187**
- nonvolatile | **2188**
- notify | **2189**

- notify-filter (Applying to the Management Target) | **2190**
- notify-filter (Configuring the Profile Name) | **2191**
- notify-view | **2192**
- oid (SNMPv3) | **2193**
- oid | **2194**
- owner | **2195**
- parameters | **2196**
- port | **2197**
- privacy-3des | **2198**
- privacy-aes128 | **2199**
- privacy-des | **2200**
- privacy-none | **2201**
- privacy-password | **2202**
- proxy (snmp) | **2203**
- read-view | **2205**
- remote-engine | **2206**
- request-type | **2208**
- request-type | **2209**
- retry-count | **2210**
- rising-event-index | **2211**
- rising-event-index | **2212**
- rising-threshold | **2213**
- rising-threshold (Health Monitor) | **2214**
- rising-threshold (RMON) | **2215**
- rmon | **2216**
- rmon | **2218**
- routing-instance | **2219**
- routing-instance-access | **2220**
- sample-type | **2221**
- sample-type | **2222**
- startup-alarm | **2223**
- security-level (Defining Access Privileges) | **2224**
- security-level (Generating SNMP Notifications) | **2225**
- security-model (Access Privileges) | **2226**

- security-model (Group) | **2227**
- security-model (SNMP Notifications) | **2228**
- security-name (Community String) | **2229**
- security-name (Security Group) | **2230**
- security-name (SNMP Notifications) | **2231**
- security-to-group | **2232**
- snmp | **2233**
- snmp-community | **2240**
- snmp-value-match-msmic (Services NAT Options) | **2241**
- source-address | **2242**
- startup-alarm | **2243**
- syslog-subtag | **2244**
- syslog-subtag | **2245**
- tag (Configuring Notification Targets) | **2246**
- tag-list | **2247**
- target-address | **2248**
- target-parameters | **2250**
- targets | **2251**
- timeout | **2252**
- traceoptions (SNMP) | **2253**
- traceoptions (SNMP) | **2256**
- trap (Security PKI) | **2258**
- trap (Security IKE) | **2260**
- trap-group | **2261**
- trap-options | **2263**
- type (RMON Notification) | **2265**
- type | **2266**
- type | **2267**
- user | **2268**
- usm | **2269**
- v3 | **2271**
- vacm | **2275**
- variable | **2276**
- variable | **2277**

- version (SNMP) | **2278**
- view (SNMP Community) | **2279**
- view (Configuring a MIB View) | **2280**
- write-view | **2281**

access (SNMP)

Syntax

```
access {
    group group-name {
        (default-context-prefix | context-prefix context-prefix) {
            security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3 vacm]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set SNMP access limits.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

access-list

Syntax

```
[edit snmp]
   routing-instance-access {
      access-list {
         routing-instance;
         routing-instance restrict;
      }
   }
```

Hierarchy Level

```
[edit snmp routing-instance-access]
```

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Create access lists to control SNMP agents in routing instances from accessing SNMP information. To enable the SNMP agent on a routing instance to access SNMP information, specify the routing instance name. To disable the SNMP agent on a routing instance from accessing SNMP information, include the routing-instance name followed by the **restrict** keyword.

Required Privilege Level

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

RELATED DOCUMENTATION

routing-instance-access | 2220

address (SNMP)

Syntax

```
address address;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the SNMP target address for receiving traps or informs.

Options

address—IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding the Implementation of SNMP on the QFabric System

Configuring SNMP | **550**

Example: Configuring SNMP | **648**

address-mask

Syntax

```
address-mask address-mask;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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 on the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Verify the source addresses for a group of target addresses.

Options

address-mask combined with the address defines a range of addresses.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Address Mask | 684

agent-address

Syntax

```
agent-address outgoing-interface;
```

Hierarchy Level

```
[edit snmp trap-options]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series and EX4600.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is **outgoing-interface**, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options

outgoing-interface—Value of the agent address of all SNMPv1 traps generated by this router or switch. The **outgoing-interface** option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: disabled (the agent address is not specified in SNMPv1 traps).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Agent Address for SNMP Traps | 590

alarm-id

Syntax

```
alarm-id id {
    alarm-state state {
        description alarm-description;
        notification-id notification-id-of-alarm;
        resource-prefix alarm-resource-prefix;
        varbind-index varbind-index-in-alarm-varbind-list;
        varbind-subtree alarm-varbind-subtree;
        varbind-value alarm-varbind-value;
    }
}
```

Hierarchy Level

```
[edit snmp alarm-management alarm-list-name]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Specify the identifier of the alarm that you need to configure.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- alarm-list-name | 2130
- alarm-management | 2131
- alarm-state | 2133

alarm (SNMP RMON)

Syntax

```
alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    request-type (get-next-request | get-request | walk-request);
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
    syslog-subtag syslog-subtag;
    variable oid-variable;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure RMON alarm entries.

Options

index—Identifies this alarm entry as an integer.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Alarm Entry and Its Attributes | **784**

event | **2025**

RMON MIB Event, Alarm, Log, and History Control Tables | **781**

Monitoring RMON MIB Tables | **642**

Understanding RMON | **774**

alarm-list-name

Syntax

```
alarm-list-name list-name {
    alarm-id  id {
        alarm-state state {
            description alarm-description;
            notification-id notification-id-of-alarm;
            resource-prefix alarm-resource-prefix;
            varbind-index varbind-index-in-alarm-varbind-list;
            varbind-subtree alarm-varbind-subtree;
            varbind-value alarm-varbind-value;
        }
    }
}
```

Hierarchy Level

```
[edit snmp alarm-management]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Specify the name of the alarm list that you need to configure.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- alarm-id | 2127
- alarm-management | 2131
- alarm-state | 2133

alarm-management

Syntax

```
alarm-management {
   alarm-list-name list-name {
      alarm-id id {
         alarm-state state {
            description alarm-description;
            notification-id notification-id-of-alarm;
            resource-prefix alarm-resource-prefix;
            varbind-index varbind-index-in-alarm-varbind-list;
            varbind-subtree alarm-varbind-subtree;
            varbind-value alarm-varbind-value;
         }
      }
   }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Configure the alarm management system to monitor and report active alarms as well as the history of alarms through the SNMP MIB tables supported by the *Alarm MIB*.

> **NOTE:** You cannot configure alarms without notifications. It is mandatory to include the notification identifier in the configuration.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

alarm-id | 2127

alarm-list-name | 2130

alarm-state | 2133

alarm-state

Syntax

```
alarm-state state {
    description alarm-description;
    notification-id notification-id-of-alarm;
    resource-prefix alarm-resource-prefix;
    varbind-index varbind-index-in-alarm-varbind-list;
    varbind-subtree alarm-varbind-subtree;
    varbind-value alarm-varbind-value;
}
```

Hierarchy Level

```
[edit snmp alarm-management alarm-list-name]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Specify the state of the alarm and the other parameters that you need to monitor.

Options

description *alarm-description*—Include a brief description of the alarm.

notification-id *notification-id-of-alarm*—Specify the identifier of the notification associated with the alarm.

resource-prefix *alarm-resource-prefix*—Specify the resource prefix of the alarm.

varbind-index *varbind-index-in-alarm-varbind-list*—Specify the varbind index in the alarm varbind list.

Range: 0 through 4294967295

varbind-subtree *alarm-varbind-subtree*—Specify the subtree of the varbind.

varbind-value *alarm-varbind-value*—Specify the varbind value of the alarm.

Range: 0 through 2147483647

Required Privilege Level

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

RELATED DOCUMENTATION

alarm-id | 2127

alarm-list-name | 2130

alarm-management | 2131

authentication-md5

Syntax

```
authentication-md5 {
    (authentication-key authentication-key | authentication-password authentication-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

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 MD5 as the authentication type for the SNMPv3 user.

NOTE: You can only configure one authentication type for each SNMPv3 user.

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MD5 Authentication | 665

authentication-none

Syntax

```
authentication-none;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure that there should be no authentication for the SNMPv3 user.

NOTE: You can configure only one authentication type for each SNMPv3 user.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring No Authentication | 666

authentication-password

Syntax

```
authentication-password authentication-password;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username authentication-md5],
[edit snmp v3 usm local-engine user username authentication-sha],
[edit snmp v3 usm remote-engine engine-id user username authentication-md5],
[edit snmp v3 usm remote-engine engine-id user username authentication-sha]
```

Release Information

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

Description

Configure the password for user authentication.

Options

authentication-password—Password that a user enters. The password is then converted into a key that is used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MD5 Authentication | 665
Configuring SHA Authentication | 666

authentication-sha

Syntax

```
authentication-sha {
    (authentication-key authentication-key | authentication-password authentication-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the secure hash algorithm (SHA) as the authentication type for the SNMPv3 user.

NOTE: You can configure only one authentication type for each SNMPv3 user.

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SHA Authentication | 666

authorization

Syntax

```
authorization authorization;
```

Hierarchy Level

```
[edit snmp community community-name]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Set the access authorization for SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests.

Options

authorization—Access authorization level:

- **read-only**—Enable **Get**, **GetNext**, and **GetBulk** requests.
- **read-write**—Enable all requests, including **Set** requests. You must configure a view to enable **Set** requests.

> **NOTE:** The **read-write** option is not supported on the QFX3000 QFabric system.

Default: read-only

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMP Community String | 577

authorization

Syntax

```
authorization authorization;
```

Hierarchy Level

```
[edit snmp community community-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.

Description

Set the access authorization for SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests.

Options

authorization—Access authorization level:

- **read-only**—Enable **Get**, **GetNext**, and **GetBulk** requests.
- **read-write**—Enable all requests, including **Set** requests. You must configure a view to enable **Set** requests.

Default: read-only

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

bucket-size

Syntax

```
bucket-size number;
```

Hierarchy Level

```
[edit snmp rmon history index]
```

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 sampling of Ethernet statistics for network fault diagnosis, planning, and performance tuning.

Default

50

Options

number—Number of discrete samples of Ethernet statistics requested.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Understanding RMON | **774**
- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON History Sampling | **791**
- Monitoring RMON MIB Tables | **642**
- *Junos OS Network Management Configuration Guide*

categories

Syntax

```
categories {
    category;
}
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Define the types of traps that are sent to the targets of the named trap group.

Default

If you omit the **categories** statement, all trap types are included in trap notifications.

Options

Categories

authentication—Authentication failures.

chassis—Chassis or environment notifications.

chassis-cluster—(For SRX Series) Clustering notifications.

configuration—Configuration notifications.

link—Link up-down transitions.

otn-alarms—OTN alarm trap subcategories.

remote-operations—Remote operations.

rmon-alarm—RMON rising and falling alarms.

routing—Routing protocol notifications.

services—Services notifications.

sonet-alarms—SONET alarm trap subcategories.

startup—System warm and cold starts.

vrrp-events—VRRP notifications.

timing-events—Timing notifications.

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | **591**

client-list

Syntax

```
client-list client-list-name {
    ip-addresses;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 8.5 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series switches and EX4600.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Define a list of SNMP clients.

Options

client-list-name—Name of the client list.

ip-addresses—IP addresses of the SNMP clients to be added to the client list,

Required Privilege Level

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

RELATED DOCUMENTATION

Adding a Group of Clients to an SNMP Community | 579

client-list-name

Syntax

```
client-list-name client-list-name;
```

Hierarchy Level

```
[edit snmp community community-name]
```

Release Information

Statement introduced in Junos OS Release 8.5 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Add a client list or prefix list to an SNMP community.

Options

client-list-name—Name of the client list or prefix list.

Required Privilege Level

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

RELATED DOCUMENTATION

Adding a Group of Clients to an SNMP Community | 579

clients

Syntax

```
clients {
   address <restrict>;
}
```

Hierarchy Level

```
[edit snmp community community community-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

Default

If you omit the **clients** statement, all SNMP clients using this community string are authorized to access the router.

Options

address—Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple ***address*** options.

restrict—(Optional) Do not allow the specified SNMP client to access the router.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

commit-delay

Syntax

```
commit-delay seconds;
```

Hierarchy Level

```
[edit snmp nonvolatile]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series switches.

Description

Configure the timer for the SNMP **Set** reply and start of the commit.

Options

seconds—Delay between an affirmative SNMP **Set** reply and start of the commit.

Default: 5 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Commit Delay Timer | 571

community (SNMP)

Syntax

```
community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
        address restrict;
    }
    view view-name;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

> **NOTE:** The **authorization read-write** option is not supported on the QFX3000 QFabric system.

The SNMP client application specifies an SNMP community name in **Get**, **GetBulk**, **GetNext**, and **Set** SNMP requests.

Default

If you omit the **community** statement, all SNMP requests are denied.

Options

community-name—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

Configuring the SNMP Community String | 577

community

Syntax

```
community community-name;
```

Hierarchy Level

```
[edit snmp rmon event index]
```

Release Information

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

Description

The trap group that is used when generating a trap (if **eventType** is configured to send traps). If that trap group has the **rmon-alarm** trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of **eventCommunity**). If nothing is configured, traps are sent to each group with the **rmon-alarm** category set.

Options

community-name—Identifies the trap group that is used when generating a trap if the event is configured to send traps.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

community (RMON)

Syntax

community *community-name*;

Hierarchy Level

[edit snmp rmon event *index*]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the SNMP trap group that is used when generating a trap (if the eventType object is configured to send traps). If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of eventCommunity). If nothing is configured, traps are sent to each group that has the rmon-alarm category configured.

The event community is not the same as an SNMP community.

Options

community-name—Name of the trap group that is used when generating a trap if the event is configured to send traps.

Required Privilege Level

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

RELATED DOCUMENTATION

RMON MIB Event, Alarm, Log, and History Control Tables | **781**

Configuring RMON Alarms and Events | **652**

Monitoring RMON MIB Tables | **642**

Understanding RMON | **774**

Junos OS Network Management Configuration Guide

community-name

Syntax

```
community-name community-name;
```

Hierarchy Level

```
[edit snmp v3 snmp-community community-index]
```

Release Information

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

Description

The community name defines an SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects.

Options

community-name—Community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose it in quotation marks (" ").

> **NOTE:** Community names must be unique. You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community *community-index*]** hierarchy levels.
>
> The community name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level is encrypted and not displayed in the command-line interface (CLI).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | 703

contact (SNMP)

Syntax

```
contact contact;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Defines the value of the SNMP MIB II **sysContact** object, which is the contact person for the managed system.

Options

contact—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the System Contact on a Device Running Junos OS | 566

customization (SNMP)

Syntax

```
customization {
    ether-stats-ifd-only;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 18.4R1.

Description

Customize SNMP behavior.

Options

ether-stats-ifd-only—Stop exposing logical interfaces (IFLs) in the etherStatsTable. When this statement is configured, the output for the **show snmp mib walk etherStatsTable** command displays data for physical interfaces (IFDs) only.

Required Privilege Level

snmp

description

Syntax

```
description description;
```

Hierarchy Level

```
[edit snmp]
```

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

Define the value of the MIB II **sysDescription** object, which is the description of the system being managed.

Options

description—System description. If the name includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the System Description on a Device Running Junos OS | 568

description

Syntax

```
description description;
```

Hierarchy Level

```
[edit snmp rmon alarm index],
[edit snmp rmon event index]
```

Release Information

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

Description

Text description of alarm or event.

Options

description—Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Description | 785
Configuring an RMON Event Entry and Its Attributes | 789

description (RMON)

Syntax

```
description description;
```

Hierarchy Level

```
[edit snmp rmon alarm index],
[edit snmp rmon event index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Text description of alarm or event.

Options

description—Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

destination-port

Syntax

```
destination-port port-number;
```

Hierarchy Level

```
[edit snmp trap-group]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Assign a trap port number other than the default.

Default

If you omit this statement, the default port is 162.

Options

port-number—SNMP trap port number.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | **591**

Configuring SNMP Trap Groups

engine-id

Syntax

```
engine-id {
   (local engine-id-suffix | use-default-ip-address | use-mac-address);
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Define a unique identifier for an SNMPv3 engine by configuring the suffix of the engine ID. The engine ID is used for identification only and not for addressing. There are two parts of an engine ID: the prefix and the suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* and cannot be configured. The suffix is configured here.

NOTE: SNMPv3 authentication and encryption keys are generated based on the associated user passwords and the engine ID. If you configure or change the engine ID, you must commit the user passwords and new engine ID before you configure SNMPv3 users, or the authentication will fail.

By default, the engine ID suffix is configured with the MAC address of the management interface (the **use-mac-address** option) on the QFX Series and OCX Series. You can override this configuration by using the **local *engine-id-suffix*** or **use-default-ip-address** option.

Default

use-mac-address

Options

local *engine-id-suffix*—The engine ID suffix is set based on the data entered.

use-default-ip-address—The engine ID suffix is generated from the default IP address.

use-mac-address—The engine ID suffix is generated from the MAC address of the management interface on the switch.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- SNMPv3 Overview (QFX in Standalone Mode) | **396**
- Configuring SNMP | **550**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

enterprise-oid

Syntax

```
enterprise-oid;
```

Hierarchy Level

```
[edit snmp trap-options]
```

Release Information
Statement introduced in Junos OS Release 10.0

Description
Add the **snmpTrapEnterprise** object, which shows the association between an enterprise-specific trap and the organization that defined the trap, to standard SNMP traps. By default, the **snmpTrapEnterprise** object is added only to the enterprise-specific traps. When the **enterprise-oid** statement is included in the configuration, **snmpTrapEnterprise** is added to all the traps generated from the device.

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

RELATED DOCUMENTATION

Configuring SNMP Trap Options | 586

event

Syntax

```
event index {
    community community-name;
    description description;
    type (RMON Notification) type;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure RMON event entries.

Options

index—Identifier for a specific event entry.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

event

Syntax

```
event index {
    community community-name;
    description description;
    type type;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

Release Information

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

Description

Configure RMON event entries.

Options

index—Identifier for a specific event entry.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

alarm (SNMP RMON) | 2022

falling-event-index

Syntax

```
falling-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

The index of the event entry that is used when a falling threshold is crossed. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a falling threshold is crossed.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Event Index or Rising Event Index | 785

rising-event-index | 2031

falling-event-index (RMON)

Syntax

```
falling-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the index number of the event entry that is used when a falling threshold is crossed. You specify the falling-event index when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a falling threshold is crossed.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

falling-threshold (Health Monitor)

Syntax

```
falling-threshold percentage;
```

Hierarchy Level

```
[edit snmp health-monitor]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

percentage—Lower threshold for the alarm entry.

Range: 1 through 100

Default: 70 percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

rising-threshold | 2214

Configuring Health Monitoring | 832

falling-threshold (RMON)

Syntax

```
falling-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the lower threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—Lower threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

Default: 20 percent less than the **rising-threshold** value

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

falling-threshold

Syntax

```
falling-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Set the lower threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—The lower threshold for the alarm entry.

Range: -2,147,483,648 through 2,147,483,647

Default: 20 percent less than **rising-threshold**

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold or Rising Threshold | 786

rising-threshold | 2032

falling-threshold-interval

Syntax

```
falling-threshold-interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Set the interval between samples after the rising threshold is exceeded and the value of the sample starts to drop. If the value of the sample drops and exceeds the falling threshold, the regular sampling interval is used.

Options

seconds—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold Interval | 787

interval | 2029

falling-threshold-interval

Syntax

```
falling-threshold-interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the interval between samples after the rising threshold is exceeded and the value of the sample starts to drop. If the value of the sample drops and exceeds the falling threshold, the regular sampling interval is used.

Options

interval—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

filter-duplicates

Syntax

```
filter-duplicates;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Filter duplicate **Get**, **GetNext**, or **GetBulk** SNMP requests.

Required Privilege Level

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

RELATED DOCUMENTATION

Filtering Duplicate SNMP Requests | **572**

Understanding the Implementation of SNMP on the QFabric System

Example: Configuring SNMP | **648**

filter-interfaces

List of Syntax

Syntax: MX, M, T, ACX, and PTX Series Routers and SRX Firewalls on page 2172
Syntax: QFX Series switches, QFabric, OCX1100 and EX4600 on page 2172

Syntax: MX, M, T, ACX, and PTX Series Routers and SRX Firewalls

```
filter-interfaces {
    interfaces {
        all-internal-interfaces;
        interface 1;
        interface 2;
    }
}
```

Syntax: QFX Series switches, QFabric, OCX1100 and EX4600

```
filter-interfaces {
    all-internal-interfaces;
    interfaces interface
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.4 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

Filter out information related to specific interfaces from the output of SNMP **Get** and **GetNext** requests performed on interface-related MIBs.

Options

all-internal-interfaces—Filters out information from SNMP **Get** and **GetNext** requests for the specified interfaces.

interfaces—Specifies the interfaces to filter out from the output of SNMP **Get** and **GetNext** requests.

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

RELATED DOCUMENTATION

Filtering Interface Information Out of SNMP Get and GetNext Output | 610

group (Defining Access Privileges for an SNMPv3 Group)

Syntax

```
group group-name;
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name security-name]
```

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Define access privileges granted to a group.

Options
group-name—Identifies a collection of SNMP security names that belong to the same access policy SNMP.

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

RELATED DOCUMENTATION

Configuring the Group | 677

group (Configuring Group Name)

Syntax

```
group group-name {
   (default-context-prefix | context-prefix context-prefiix){
      security-model (any | usm | v1 | v2c) {
         security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
         }
      }
   }
}
```

Hierarchy Level

```
[edit snmp v3 vacm access]
```

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

Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The **default-context-prefix** statement, when included, adds all the contexts configured on the device to the group, whereas the **context-prefix *context-prefix*** statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series and OCX Series.) When the context prefix is specified as default (for example, **context-prefix default**), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as **logical system/routing instance**. For example, to specify routing instance ri1 in logical system ls1, include **context-prefix ls1/ri1**.

The remaining statements under this hierarchy are explained separately.

Options

group-name—SNMPv3 group name created for the SNMPv3 group.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring the Group | 671

health-monitor

Syntax

```
health-monitor {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
}
```

Hierarchy Level

[edit snmp]

Release Information
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure health monitoring.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring Health Monitoring | 832
Understanding Health Monitoring | 831

history

Syntax

```
history history-index {
    bucket-size number;
    interface interface-name;
    interval seconds;
    owner owner-name;
}
```

Hierarchy Level

```
[edit snmp rmon]
```

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 RMON history group entries. This RMON feature can be used with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments. The RMON history feature collects statistics in accordance with user-configurable parameters.

The history group controls the periodic statistical sampling of data from various types of networks. This group contains configuration entries that specify an interface, polling period, and other parameters. If you use the **history** statement, you must also configure the **interface *interface-name*** statement.

Default

Not configured.

Options

history-index—Tag the history entries with a number.

Range: 1 through 655535 (integer)

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding RMON | 774

RMON MIB Event, Alarm, Log, and History Control Tables | 781

Configuring RMON History Sampling | 791

Monitoring RMON MIB Tables | 642

Junos OS Network Management Configuration Guide

interface (SNMP)

Syntax

```
interface [ interface-names ];
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the interfaces on which SNMP requests can be accepted.

Default

If you omit this statement, SNMP requests entering the router or switch through any interface are accepted.

Options

interface-names—Names of one or more logical interfaces.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interfaces on Which SNMP Requests Can Be Accepted | 609

interface (SNMP RMON History)

Syntax

```
interface interface-name;
```

Hierarchy Level

```
[edit snmp rmon history history-index]
```

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

Specify the interface to be monitored in the specified RMON history entry.

Only one interface can be specified for a particular RMON history index. There is a one-to-one relationship between the interface and the history index. The interface must be specified in order for the RMON history to be created.

Options

interface-name—Specify the interface to be monitored within the specified entry of the RMON history of Ethernet statistics.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Understanding RMON | **774**
- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON History Sampling | **791**
- Monitoring RMON MIB Tables | **642**
- *Junos OS Network Management Configuration Guide*

interval

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Interval between samples.

Options

seconds—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Interval | 786

interval (Health Monitor)

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp health-monitor]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the interval between sampling of the object being monitored by the health monitor.

Options

seconds—Time between samples, in seconds.

Range: **1** through **2147483647** seconds

Default: **300** seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Health Monitoring | 832

interval (SNMP RMON)

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp rmon alarm index],
[edit snmp rmon history]
```

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 interval over which data is to be sampled for the specified interface.

Default

60 sec for alarm sampling.

1800 sec for Ethernet packet history sampling.

Options

seconds—Interval at which data is to be sampled for the specified interface.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Understanding RMON | **774**
- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON History Sampling | **791**
- Monitoring RMON MIB Tables | **642**

local-engine

Syntax

```
local-engine {
    user username {
        authentication-md5 {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        authentication-none;
        authentication-sha {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        privacy-aes128 {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-3des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-none {
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3 usm]
```

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 local engine information for the user-based security model (USM).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

location (SNMP)

Syntax

```
location location;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the value of the MIB II **sysLocation** object, which is the physical location of the managed system.

Options

location—Location of the local system. You must enclose the name within quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the System Location for a Device Running Junos OS | 567

logical-system

Syntax

```
logical-system logical-system-name {
    routing-instance routing-instance-name {
        source-address address;
    }
}
```

Hierarchy Level

```
[edit snmp community community-name],
[edit snmp trap-group],
[edit snmp trap-options]
[edit snmp v3target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 9.3
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

> **NOTE:** The **logical-system** statement replaces the **logical-router** statement, and is backward-compatible with Junos OS Release 8.3 and later.

Description

Specify a logical system name for SNMP v1 and v2c clients.

Include at the **[edit snmp trap-options]** hierarchy level to specify a logical-system address as the source address of an SNMP trap.

Include at the **[edit snmp v3 target-address]** hierarchy level to specify a logical-system name as the destination address for an SNMPv3 trap or inform.

Options

logical-system-name–Name of the logical system.

routing-instance *routing-instance-name*–Statement to specify a routing instance associated with the logical system.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728
Configuring the Trap Target Address | 683

logical-system-trap-filter

Syntax

```
logical-system-trap-filter;
```

Hierarchy Level

```
[edit snmp]
```

Release Information
Statement introduced in Junos OS Release 8.4.

Description
Restrict the routing instances from receiving traps that are not related to the logical system networks to which they belong.

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

RELATED DOCUMENTATION

SNMP Traps Supported for Routing Instances | 726

message-processing-model

Syntax

```
message-processing-model (v1 | v2c | v3);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameter-name parameters]
```

Release Information

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

Description

Configure the message processing model to be used when generating SNMP notifications.

Options

v1—SNMPv1 message process model.

v2c—SNMPv2c message process model.

v3—SNMPv3 message process model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Message Processing Model | 690

name

Syntax

```
name name;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Set the system name from the command-line interface.

Options

name—System name override.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a Different System Name | 571

nonvolatile

Syntax

```
nonvolatile {
    commit-delay seconds;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
The **commit-delay** statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure options for SNMP **Set** requests.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Commit Delay Timer | 571

commit-delay | 2147

notify

Syntax

```
notify name {
   tag tag-name;
   type (trap | inform);
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

Statement introduced before Junos OS Release 7.4.
type inform option added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.

Options

name—Name assigned to the notification.

tag-name—Notifications are sent to all targets configured with this tag.

type—Notification type is **trap** or **inform**. Traps are unconfirmed notifications. Informs are confirmed notifications.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Inform Notification Type and Target Address | 693
Configuring the SNMPv3 Trap Notification | 680

notify-filter (Applying to the Management Target)

Syntax

```
notify-filter profile-name;
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the notify filter to be used by a specific set of target parameters.

Options

profile-name—Name of the notify filter to apply to notifications.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying the Trap Notification Filter | 689

notify-filter (Configuring the Profile Name)

Syntax

```
notify-filter profile-name {
    oid oid (include | exclude);
}
```

Hierarchy Level

```
[edit snmp v3]
```

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

Specify a group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.

Options

profile-name—Name assigned to the notify filter.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Notification Filter | 682
oid (SNMPv3) | 2193

notify-view

Syntax

```
notify-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
```

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

Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—Name of the view to which the SNMP user group has access.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MIB Views | **612**
Configuring the Notify View | **673**

oid (SNMPv3)

Syntax

```
oid oid <include | exclude>;
```

Hierarchy Level

```
[edit snmp v3 notify-filter profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify an object identifier (OID) used to represent a subtree of MIB objects. This OID is a prefix that the represented MIB objects have in common.

Default

include. The subtree of MIB objects represented by the specified OID is included.

Options

exclude—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

oid—Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

Required Privilege Level

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

RELATED DOCUMENTATION

SNMPv3 Overview (QFX in Standalone Mode) | **396**

Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

Configuring SNMP | **550**

Configuring the Trap Notification Filter | 682

oid

Syntax

```
oid object-identifier <exclude | include>;
```

Hierarchy Level

```
[edit snmp view view-name]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, OCX switches and SRX devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify an object identifier (OID) used to represent a subtree of MIB objects.

Default
include. The subtree of MIB objects represented by the specified OID is included.

Options
exclude—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

RELATED DOCUMENTATION

Configuring MIB Views | 612

owner

Syntax

```
owner owner-name;
```

Hierarchy Level

```
[edit snmp rmon history]
```

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

Specify the user or group responsible for this RMON history configuration.

Options

owner-name—The user or group responsible for this configuration.

Range: 0 through 32 alphanumeric characters

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Understanding RMON | **774**
- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON History Sampling | **791**
- Monitoring RMON MIB Tables | **642**

parameters

Syntax

```
parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (none | authentication | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
}
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-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.

Description

Configure a set of target parameters for message processing and security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining and Configuring the Trap Target Parameters | 688

port

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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.

Description

Configure a UDP port number for an SNMP target.

Default

If you omit this statement, the default port is 162.

Options

port-number—Port number for the SNMP target.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Port | 685

privacy-3des

Syntax

```
privacy-3des {
   (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-aes128

Syntax

```
privacy-aes128 {
    (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-des

Syntax

```
privacy-des {
    (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-none

Syntax

```
privacy-none;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

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 that no encryption be used for the SNMPv3 user.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-password

Syntax

```
privacy-password privacy-password;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username privacy-3des],
[edit snmp v3 usm local-engine user username privacy-aes128],
[edit snmp v3 usm local-engine user username privacy-des],
[edit snmp v3 usm remote-engine engine-id user username privacy-3des],
[edit snmp v3 usm remote-engine engine-id user username privacy-aes128],
[edit snmp v3 usm remote-engine engine-id user username privacy-des]
```

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 a privacy password for the SNMPv3 user.

Options

privacy-password—Password that a user enters. The password is then converted into a key that is used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

proxy (snmp)

Syntax

```
proxy proxy-name{
    device-name device-name;
    logical-system logical-system {
        routing-instance routing-instance;
    }
    routing-instance routing-instance;
    (version-v1 | version-v2c) {
        snmp-community community-name;
        no-default-comm-to-v3-config;
    }
    version-v3 {
        security-name security-name;
        context context-name;
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Configure a device to act as a proxy SNMP agent, and specify a name for the proxy.

Options

context *context-name*—Specify the SNMPv3 context name as configured on the device specified at **edit snmp proxy *proxy-name* device-name *device-name***.

For more information about this statement, see **context**.

device-name *device-name*—Specify the name of the device to be managed through the proxy SNMP agent.

no-default-comm-to-v3-config—(Optional) Specify whether you have to manually configure the statements at the **[edit snmp v3 snmp-community *community-name*]** and **[edit snmp v3 vacm]** hierarchy levels.

If this statement is not included in the configuration, the **[edit snmp v3 snmp-community *community-name*]** and **[edit snmp v3 vacm]** hierarchy level configurations are automatically initialized.

proxy-name—Specify the name of the proxy.

security-name *security-name*—Specify the SNMPv3 security name as configured on the device specified at **edit snmp proxy *proxy-name* device-name *device-name***.

For more information about this statement, see **security-name**.

snmp-community *community-name*—Specify the name of the SNMP community. The community name you configure should match the **snmp-community** configuration on the device specified at **edit snmp proxy *proxy-name* device-name *device-name***. For more information about this statement, see **snmp-community**.

(version-v1 | version-v2c)—Specify the SNMP version, and add the relevant configuration.

version-v3—Add the SNMPv3 configuration.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a Proxy SNMP Agent | **581**

read-view

Syntax

```
read-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
```

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

Associate the read-only view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—The name of the view to which the SNMP user group has access.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Read View | **674**

Configuring MIB Views | **612**

remote-engine

Syntax

```
remote-engine engine-id {
    user username {
        authentication-md5 {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        authentication-none;
        authentication-sha {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        privacy-aes128 (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-3des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-none {
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3 usm]
```

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.

Options

engine-id—Specify engine identifier in hexadecimal format. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring the Remote Engine and Remote User | 696

request-type

Syntax

```
request-type (get-next-request | get-request | walk-request);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Extend monitoring to a specific SNMP object instance (get-request), to all object instances belonging to a MIB branch (walk-request), or to the next object instance after the instance specified in the configuration (get-next-request).

Default

walk-request

Options

get-next-request—Perform an SNMP get next request.

get-request—Perform an SNMP get request.

walk-request—Perform an SNMP walk request.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

request-type

Syntax

```
request-type (get-next-request | get-request | walk-request);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Extend monitoring to a specific SNMP object instance (**get-request**), or extend monitoring to all object instances belonging to a MIB branch (**walk-request**), or extend monitoring to the next object instance after the instance specified in the configuration (**get-next-request**).

Options

get-next-request—Performs an SNMP get next request.

get-request—Performs an SNMP get request.

walk-request—Performs an SNMP walk request.

Default: walk-request

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Request Type | 787

variable | 2038

retry-count

Syntax

```
retry-count number;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Configure the retry count for SNMP informs.

Options

number—Maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.

Default: 3 times

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Informs | 692

timeout | 2298

rising-event-index

Syntax

```
rising-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the index of the event entry that is used when a rising alarm threshold is exceeded. The rising-event index is specified when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a rising threshold is exceeded.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

rising-event-index

Syntax

```
rising-event-index index;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Index of the event entry that is used when a rising threshold is crossed. If this value is zero, no event is triggered.

Options

index—Index of the event entry that is used when a rising threshold is crossed.

Range: 0 through 65,535

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Event Index or Rising Event Index | 785

falling-event-index | 2026

rising-threshold

Syntax

```
rising-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Set the upper threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—The lower threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Falling Threshold or Rising Threshold | 786

falling-threshold | 2027

rising-threshold (Health Monitor)

Syntax

```
rising-threshold percentage;
```

Hierarchy Level

```
[edit snmp health-monitor]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

percentage—Upper threshold for the alarm entry.

Range: **1** through **100**

Default: **80** percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Health Monitoring | **832**

falling-threshold | **2166**

rising-threshold (RMON)

Syntax

```
rising-threshold integer;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the upper threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

integer—Upper threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

rmon

Syntax

```
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type;
        rising-event-index index;
        rising-threshold integer;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type (RMON Notification) type;
    }
    history history-index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Provide comprehensive network fault diagnosis, planning, and performance tuning information. RMON delivers this information in nine groups of monitoring elements, each providing specific sets of data to

meet common network monitoring requirements. Each group is optional, so that vendors do not need to support all the groups within the MIB.

Junos OS supports the RMON statistics, history, alarm, and event groups.

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

rmon

Syntax

```
rmon { ... }
```

Hierarchy Level

```
[edit snmp]
```

Release Information

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

Description

Configure Remote Monitoring.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Alarm Entry and Its Attributes | 784

routing-instance

Syntax

```
routing-instance routing-instance-name {
    source-address address;
}
```

Hierarchy Level

```
[edit snmp community community-name],
[edit snmp community community-name logical-system logical-system-name],
[edit snmp trap-group group],
[edit snmp trap-options]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Added to the **[edit snmp community *community-name*]** hierarchy level in Junos OS Release 8.4.
Added to the **[edit snmp community *community-name* logical-system *logical-system-name*]** hierarchy level in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

Specify a routing instance for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use this routing instance.

If the routing instance is defined within a logical system, include the **logical-system *logical-system-name*** statement at the **[edit snmp community *community-name*]** hierarchy level and specify the **routing-instance** statement under the **[edit snmp community *community-name* logical-system *logical system-name*]** hierarchy level.

Options

routing-instance-name—Name of the routing instance.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | **591**

Configuring the Source Address for SNMP Traps | **587**

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community | 728

routing-instance-access

Syntax

```
[edit snmp]
   routing-instance-access {
      access-list {
         routing-instance;
         routing-instance restrict;
      }
   }
```

Hierarchy Level

```
[edit snmp]
```

Release Information
Statement introduced in Junos OS Release 8.4.

Description
Enable SNMP managers in routing instances other than the default routing instance to access SNMP information. For information about the **access-list** option, see **access-list**.

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

RELATED DOCUMENTATION

Enabling SNMP Access over Routing Instances | 727

sample-type

Syntax

```
sample-type (absolute-value | delta-value);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the method of sampling the selected variable (monitored object). When you configure an SNMP RMON alarm, you can specify the sample type.

Options

absolute-value—Actual value of the selected variable is used when comparing against the thresholds.

delta-value—Difference between samples of the selected variable is used when comparing against the thresholds.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

sample-type

Syntax

```
sample-type (absolute-value | delta-value);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Method of sampling the selected variable.

Options

absolute-value—Actual value of the selected variable is used when comparing against the thresholds.

delta-value—Difference between samples of the selected variable is used when comparing against the thresholds.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Sample Type | 787

startup-alarm

Syntax

```
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

The alarm that can be sent upon entry startup.

Options

falling-alarm—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.

rising-alarm—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.

rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

Default: rising-or-falling-alarm

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Startup Alarm | 788

security-level (Defining Access Privileges)

Syntax

```
security-level (authentication | none | privacy) {
    notify-view view-name;
    read-view view-name;
    write-view view-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c)]
```

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

Define the security level used for access privileges.

Default

none

Options

authentication—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Level | 672

security-level (Generating SNMP Notifications)

Syntax

```
security-level (authentication | none | privacy);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security level to use when generating SNMP notifications.

Default

none

Options

authentication—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Level | 691

security-model (Access Privileges)

Syntax

```
security-model (usm | v1 | v2c);
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)]
```

Release Information

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

Description

Configure the security model for an SNMPv3 group. The security model is used to determine access privileges for the group.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 671

security-model (Group)

Syntax

```
security-model (usm | v1 | v2c) {
    security-name security-name {
        group group-name;
    }
}
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group]
```

Release Information

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

Description

Define a security model for a group.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 676

security-model (SNMP Notifications)

Syntax

```
security-model (usm | v1 | v2c);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security model for an SNMPv3 group. The security model is used for SNMP notifications.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 690

security-name (Community String)

Syntax

```
security-name security-name;
```

Hierarchy Level

```
[edit snmp v3 snmp-community community-index]
```

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

Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Options

security-name—Name that is used for messaging security and user access control.

> **NOTE:** The security name must match the configured security name at the **[edit snmp v3 target-parameters *target-parameters-name* parameters]** hierarchy level when you configure traps or informs.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Names | 705

security-name (Security Group)

Syntax

```
security-name security-name {
    group group-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
```

Release Information

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

Description

Associate a group or a community string with a configured security group.

Options

security-name—Username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Assigning Security Names to Groups | 677

security-name (SNMP Notifications)

Syntax

```
security-name security-name;
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security name used when generating SNMP notifications.

Options

security-name—If the SNMPv3 USM security model is used, identify the user when generating the SNMP notification. If the v1 or v2c security models are used, identify the SNMP community used when generating the notification.

> **NOTE:** The access privileges for the group associated with this security name must allow this notification to be sent.
>
> If you are using the v1 or v2 security models, the security name at the **[edit snmp v3 vacm security-to-group]** hierarchy level must match the security name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Name | 691

security-to-group

Syntax

```
security-to-group {
    security-model (usm | v1 | v2c) {
        group group-name;
        security-name security-name;
    }
}
```

Hierarchy Level

```
[edit snmp v3 vacm]
```

Release Information

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

Description

Configure the group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Assigning Security Model and Security Name to a Group | 676

snmp

List of Syntax

Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches on page 2233
Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600 on page 2233

Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches

```
snmp { ... }
```

Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600

```
snmp {
    client-list client-list-name {
        ip-addresses;
    }
    community community-name {
        authorization authorization;
        client-list-name client-list-name;
        clients {
            address restrict;
        }
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                clients {
                addresses;
                }
            }
        }
        routing-instance routing-instance-name {
            clients {
            addresses;
            }
        }
        view view-name;
    }
    contact contact;
    description description;
    filter-duplicates;
    filter-interfaces;
    health-monitor {
        falling-threshold integer;
        interval seconds;
        rising-threshold integer;
```

```
}
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type;
        rising-event-index index;
        rising-threshold integer;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
    history history-index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regular-expression>;
    flag flag;
}
```

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
```

```
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance routing-instance-name;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);
            security-model (usm | v1 | v2c);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-sha {
                    authentication-password authentication-password;
                }
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-none;
                privacy-aes128 {
```

```
            privacy-password privacy-password;
          }
          privacy-des {
            privacy-password privacy-password;
          }
          privacy-3des {
            privacy-password privacy-password;
          }
          privacy-none;
        }
      }
      remote-engine engine-id {
        user username {
          authentication-sha {
            authentication-password authentication-password;
          }
          authentication-md5 {
            authentication-password authentication-password;
          }
          authentication-none;
          privacy-aes128 {
            privacy-password privacy-password;
          }
          privacy-des {
            privacy-password privacy-password;
          }
          privacy-3des {
            privacy-password privacy-password;
          }
          privacy-none {
            privacy-password privacy-password;
          }
        }
      }
    }
```

```
    vacm {
      access {
        group group-name {
          (default-context-prefix | context-prefix context-prefix) {
            security-model (any | usm | v1 | v2c) {
              security-level (authentication | none | privacy) {
                notify-view view-name;
                read-view view-name;
                write-view view-name;
              }
            }
          }
        }
      }
      security-to-group {
        security-model (usm | v1 | v2c) {
          security-name security-name {
            group group-name;
          }
        }
      }
    }
  }
  view view-name {
    oid object-identifier (include | exclude);
  }
}
}
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure SNMP.

SNMP modules cannot have the slash (/) character or the @ character in the name.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Configuring SNMP on a Device Running Junos OS | **564**
- Understanding SNMP Implementation in Junos OS | **389**
- Configuring SNMP | **550**

snmp-community

Syntax

```
snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}
```

Hierarchy Level

```
[edit snmp v3]
```

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 SNMP community.

Options

community-index—(Optional) String that identifies an SNMP community.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | 703

snmp-value-match-msmic (Services NAT Options)

Syntax

```
snmp-value-match-msmic;
```

Hierarchy Level

```
[edit services service-set service-set-name nat-options]
```

Release Information

Statement introduced with Junos OS Release 13.3R7

Description

Match the values for MS-MIC-specific objects in the jnxNatObjects MIB table with the values for MS-DPC objects. Use the **deactivate services service-set *service-set-name* nat-options snmp-value-match-msmic** configuration mode command to disable this feature. By default, this feature is disabled.

Required Privilege Level

control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Service Rules

Troubleshooting the Mismatch of jnxNatObjects Values for MS-DPC and MS-MIC | **1622**

source-address

Syntax

```
source-address address;
```

Hierarchy Level

```
[edit snmp trap-options]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, SRX devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the source address of every SNMP trap packet sent by this router to a single address regardless of the outgoing interface. If the source address is not specified, the default is to use the address of the outgoing interface as the source address.

Options

address—Source address of SNMP traps. You can configure the source address of trap packets two ways: **lo0** or a valid IPv4 address configured on one of the router interfaces. The value **lo0** indicates that the source address of all SNMP trap packets is set to the lowest loopback address configured at interface **lo0**.

Default: Disabled. (The source address is the address of the outgoing interface.)

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Source Address for SNMP Traps | 587

startup-alarm

Syntax

```
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set an initial alarm that is sent after the configured SNMP RMON alarm becomes active.

Default

rising-or-falling-alarm

Options

falling-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the falling threshold.

rising-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the rising threshold.

rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active is equal to or greater than either the rising threshold or the falling threshold.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Configuring RMON Alarms and Events | **652**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

syslog-subtag

Syntax

```
syslog-subtag syslog-subtag;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Add the **syslog-subtag** tag to the system log message. The tag should not exceed 80 uppercase characters.

Required Privilege Level

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

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Understanding RMON | **774**
- *Junos OS Network Management Configuration Guide*

syslog-subtag

Syntax

```
syslog-subtag syslog-subtag;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Add a tag to the system log message.

Options

syslog-subtag *syslog-subtag*—Tag of not more than 80 uppercase characters to be added to syslog messages.

Default: None

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the System Log Tag | 788

tag (Configuring Notification Targets)

Syntax

```
tag tag-name;
```

Hierarchy Level

```
[edit snmp v3 notify name]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure a set of target addresses to receive SNMP traps or informs (for IPv4 packets only).

Options

tag-name—Define the target addresses to which an SNMP notification is sent. Target addresses containing the same tag in their tag list are sent the same notification. The ***tag-name*** is not included in the notification.

Required Privilege Level

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

RELATED DOCUMENTATION

- SNMPv3 Overview (QFX in Standalone Mode) | **396**
- Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**
- Configuring SNMP | **550**
- Configuring the SNMPv3 Trap Notification | **680**

tag-list

Syntax

```
tag-list tag-list;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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.

Description

Configure an SNMP tag list used to select target addresses.

Options

tag-list—Define sets of target addresses (tags). To specify more than one tag, specify the tag names as a space-separated list enclosed within double quotes.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Target Address | 685

target-address

Syntax

```
target-address target-address-name {
    address address;
    address-mask address-mask;
    port port-number;
    retry-count number;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the address of an SNMP management application and the parameters to be used in sending notifications.

Options

target-address-name—String that identifies the target address.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- SNMP MIBs Support | **616**
- SNMP Traps Support | **594**
- snmp | **2233**
- Configuring SNMP | **550**

show snmp | 399

Example: Configuring SNMP | 648

target-parameters

Syntax

At the **[edit snmp v3]** hierarchy level:

```
target-parameters target-parameters-name {
    profile-name;
    parameters {
        message-processing-model (v1 | v2c | V3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
```

At the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
target-parameters target-parameters-name;
```

Hierarchy Level

```
[edit snmp v3]
[edit snmp v3 target-address target-address-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.

Description

Configure the message processing and security parameters for sending notifications to a particular management target. The target parameters are configured at the **[edit snmp v3]** hierarchy level. The remaining statements at this level are explained separately.

Then apply the target parameters configured at the **[edit snmp v3 target-parameters *target-parameters-name*]** hierarchy level to the target address configuration at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining and Configuring the Trap Target Parameters | 688
Applying Target Parameters | 686

targets

Syntax

```
targets {
    address;
}
```

Hierarchy Level

[edit snmp trap-group *group-name*]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure one or more systems to receive SNMP traps.

Options

address—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | 591
Configuring SNMP Trap Groups

timeout

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the timeout period (in seconds) for SNMP informs.

Default

15 seconds

Options

seconds—Number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding SNMP Implementation in Junos OS | **389**
- Configuring SNMP Informs | **692**
- retry-count | **2210**

traceoptions (SNMP)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Track the activities of SNMP agents on the switch and record the information in log files.

> **NOTE:** The **traceoptions** statement is not supported on the QFabric system.

The output of the tracing operations is placed into log files in the **/var/log** directory. Each log file is named after the SNMP agent that generates it. The following logs are created in the **/var/log** directory when the **traceoptions** statement is used:

- chassisd
- craftd
- ilmid
- mib2d
- rmopd
- serviced
- snmpd

Options

file *filename*—By default, the name of the log file that records trace output is the name of the process being traced (for example, mib2d or snmpd). Use this option to specify another name.

files *number*—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, snmpd) reaches its maximum size, it is archived by being renamed to snmpd.0. The previous snmpd.1 is renamed to snmpd.2, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements:

- **all**—Log all SNMP events.
- **configuration**—Log reading of configuration at the **[edit snmp]** hierarchy level.
- **database**—Log events involving storage and retrieval in the events database.
- **events**—Log important events.
- **general**—Log general events.
- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **policy**—Log policy processing.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **server**—Log communication with processes that are generating events.
- **subagent**—Log subagent restarts.
- **timer-events**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

Range: 10 KB through 1 GB

Default: 1000 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Tracing and Logging Operations | 9

Tracing SNMP Activity on a Device Running Junos OS | 766

traceoptions (SNMP)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
file *filename* option added in Junos OS Release 8.1.
world-readable | no-world-readable option added in Junos OS Release 8.1.
match *regular-expression* option added in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

The output of the tracing operations is placed into log files in the **/var/log** directory. Each log file is named after the SNMP agent that generates it. Currently, the following logs are created in the **/var/log** directory when the **traceoptions** statement is used:

- chassisd
- craftd
- ilmid
- mib2d
- rmopd
- serviced
- snmpd

Options

file *filename*—By default, the name of the log file that records trace output is the name of the process being traced (for example, **mib2d** or **snmpd**). Use this option to specify another name.

files *number*—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, **snmpd**) reaches its maximum size, it is archived by being renamed to **snmpd.0**. The previous **snmpd.1** is renamed to **snmpd.2**, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements:

- **all**—Log all SNMP events.
- **general**—Log general events.
- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **subagent**—Log subagent restarts.
- **timer**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

Range: 10 KB through 1 GB

Default: 1000 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

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

RELATED DOCUMENTATION

Tracing SNMP Activity on a Device Running Junos OS | **766**

trap (Security PKI)

Syntax

```
trap {
    all certificates number-of-days;
    ca-identity number-of-days;
    certificate-id number-of-days;
}
```

Hierarchy Level

```
[edit security pki]
```

Release Information
Statement introduced in Junos OS Release 20.1R1

Description
To configure certificate expiration trap and configure the number of days before to generate the trap.

how

Default

- **all certificates**—60 days
- **ca-identity**—60 days
- **certificate-id** —60 days

Options

all certificates ***number-of-days*** —Number of days to generate traps for all certificates. You can configure from *1 to 100* days.

ca-identity ***number-of-days*** —Number of days to generate traps for specified CA certificate. You can configure from *1 to 100* days.

certificate-id ***number-of-days*** —Number of days to generate for specified local certificate. You can configure from *1 to 100* days.

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

RELATED DOCUMENTATION

- Configure the Certificate Expiration Trap | **770**
- Enable Peer Down and IPsec Tunnel Down Traps | **772**
- *show security ipsec statistics*

trap (Security IKE)

Syntax

```
trap {
   ipsec-tunnel-down ;
   peer-down ;
}
```

Hierarchy Level

```
[edit security ike trap]
```

Release Information

Statement introduced in Junos OS Release 20.1R1

Description

ipsec-tunnel-down— By enabling the **ipsec-tunnel-down** option, the traps are generated for IPsec tunnel going down only when the associated peer IKE SA is up.

peer-down—By enabling the **peer-down** option, the traps are generated when peer goes down. Traps for the corresponding IPsec tunnels going down for the peer are not generated.

Default

- **peer-down**—Disabled
- **ipsec-tunnel-down**—Disabled

Required Privilege Level

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

RELATED DOCUMENTATION

Configure the Certificate Expiration Trap | **770**

Enable Peer Down and IPsec Tunnel Down Traps | **772**

show security ipsec statistics

trap-group

List of Syntax

Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls on page 2261
Syntax: QFX and EX Series Switches and OCX1100 on page 2261

Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
    targets {
        address;
    }
    version (all | v1 | v2);
}
```

Syntax: QFX and EX Series Switches and OCX1100

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    targets {
        address;
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, and SRX and vSRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series switches.

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

Options

group-name—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | **591**

Configuring SNMP Trap Groups

trap-options

List of Syntax

Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls on page 2263
QFX Series Switches, EX4600, OCX1100 on page 2263

Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls

```
trap-options {
    agent-address outgoing-interface;
    context-oid;
    enterprise-oid;
    logical-system logical-system-name {
        routing-instance routing-instance-name {
            source-address address;
        }
    }
    routing-instance routing-instance-name {
        source-address address;
    }
}
```

QFX Series Switches, EX4600, OCX1100

```
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers, and SRX Firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
context-oid option introduced in Junos OS Release 17.1.

Description

Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.

Default

Disabled

Options

context-oid—Add context oid in varbind of all traps originating from non-default logical system and routing instance. If your network management system is not able to handle prefixes such as **<routing-instance name>@<trap-group-name>** or **<logical-system name>/<routing-instance name>@<trap-group-name>**, setting the **context-oid** configuration statement will send only the **<trap-group-name>** and add **<logical-system name>/<routing-instance name>** as an additional varbind.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Options | 586

type (RMON Notification)

Syntax

```
type type;
```

Hierarchy Level

```
[edit snmp rmon event index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the type of notification generated when a rising or falling threshold is crossed.

Default

log-and-trap

Options

type—Type of notification. It can be one of the following:

- **log**—Add an entry to the **logTable** object.
- **log-and-trap**—Send an SNMP trap and add a log entry.
- **none**—No notifications are sent.
- **snmptrap**—Send an SNMP trap.

Required Privilege Level

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

RELATED DOCUMENTATION

RMON MIB Event, Alarm, Log, and History Control Tables | **781**

Configuring RMON Alarms and Events | **652**

Monitoring RMON MIB Tables | **642**

Understanding RMON | **774**

Junos OS Network Management Configuration Guide

type

Syntax

```
type type;
```

Hierarchy Level

```
[edit snmp rmon event index]
```

Release Information

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

Description

Type of notification generated when a threshold is crossed.

Options

type—Type of notification:

- **log**—Add an entry to **logTable**.
- **log-and-trap**—Send an SNMP trap and make a log entry.
- **none**—No notifications are sent.
- **snmptrap**—Send an SNMP trap.

Default: log-and-trap

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an RMON Event Entry and Its Attributes | 789

type

Syntax

```
type (inform | trap);
```

Hierarchy Level

```
[edit snmp v3 notify name]
```

Release Information

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

Description

Configure the type of SNMP notification.

Options

inform—Defines the type of notification as an inform. SNMP informs are confirmed notifications.

trap—Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Informs | 692

Configuring the SNMPv3 Trap Notification | 680

user

Syntax

```
user username;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine],
[edit snmp v3 usm remote-engine engine-id]
```

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

Specify a user associated with an SNMPv3 group on a local or remote SNMP engine.

Options

username—SNMPv3 user-based security model (USM) username.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

usm

Syntax

```
usm {
    local-engine {
        user username {
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none {
                privacy-password privacy-password;
            }
        }
        remote-engine engine-id {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-none;
                authentication-sha {
                    authentication-password authentication-password;
                }
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-3des {
                    privacy-password privacy-password;
                }
```

```
            privacy-none {
               privacy-password privacy-password;
            }
         }
      }
   }
}
```

Hierarchy Level

```
[edit snmp v3]
```

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 user-based security model (USM) information.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

Configuring the Remote Engine and Remote User | 696

v3

Syntax

```
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        port port-number;
        retry-count number;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);
            security-model (usm | v1 | v2c);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-sha {
                    authentication-password authentication-password;
                }
                authentication-none;
```

```
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none;
        }
    }
    remote-engine engine-id {
        user username {
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-sha {
                authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none {
                privacy-password privacy-password;
            }
        }
    }
}
```

```
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix) {
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c) {
            security-name security-name {
                group group-name;
            }
        }
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure SNMPv3.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

vacm

Syntax

```
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix){
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c);
        security-name security-name {
            group group-name;
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

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

Description

Configure view-based access control model (VACM) information.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining Access Privileges for an SNMP Group | 669

variable

Syntax

```
variable oid-variable;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Set the object identifier (OID) of the MIB object (also called variable) to be monitored when you configure an SNMP RMON alarm. If the value of the monitored variable exceeds the configured rising threshold or falling threshold, an alarm is triggered and a corresponding event may be generated.

Options

oid-variable—OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, **1.3.6.1.2.1.2.1.2.2.1.10.1**) or the name of the MIB object—for example, **ifInOctets.1**.

Required Privilege Level

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

RELATED DOCUMENTATION

RMON MIB Event, Alarm, Log, and History Control Tables | 781

Configuring RMON Alarms and Events | 652

Monitoring RMON MIB Tables | 642

Understanding RMON | 774

Junos OS Network Management Configuration Guide

variable

Syntax

```
variable oid-variable;
```

Hierarchy Level

```
[edit snmp rmon alarm index]
```

Release Information

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

Description

Object identifier (OID) of MIB variable to be monitored.

Options

oid-variable—OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, **1.3.6.1.2.1.2.1.2.2.1.10.1**). Alternatively, use the MIB object name (for example, **ifInOctets.1**).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Variable | 789

version (SNMP)

Syntax

```
version (all | v1 | v2);
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, EX Series switches and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX4600 switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX1100 switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the version number of SNMP traps.

Default

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options

all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups | 591

Configuring SNMP Trap Groups

view (SNMP Community)

Syntax

```
view view-name;
```

Hierarchy Level

```
[edit snmp community community-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX4600 switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX1100.

Description

Associate a view with a community. A view represents a group of MIB objects.

Options

view-name—Name of the view. You must use a view name already configured in the **view** statement at the **[edit snmp]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Communities | 573

view (Configuring a MIB View)

Syntax

```
view view-name {
    oid object-identifier (include | exclude);
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The **view** statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the **view** statement at the **[edit snmp community *community-name*]** hierarchy level.

> **NOTE:** To remove an OID completely, use the **delete view all oid oid-number** command but omit the **include** parameter.

Options

view-name—Name of the view.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MIB Views | 612

Associating MIB Views with an SNMP User Group | 672

community | 2148

write-view

Syntax

```
write-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level  (authentication | none | privacy)]
```

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 switches.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—Name of the view for which the SNMP user group has write permission.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MIB Views | 612

Configuring the Write View | 674

CHAPTER 72

Configuration Statements: SNMPv3

IN THIS CHAPTER

- address | 2284
- address-mask | 2285
- authentication-key | 2286
- authentication-md5 | 2287
- authentication-none | 2288
- authentication-password | 2289
- authentication-sha | 2290
- community-name | 2291
- context (SNMPv3) | 2292
- engine-id | 2293
- group (Configuring Group Name) | 2295
- group (Defining Access Privileges for an SNMPv3 Group) | 2296
- retry-count | 2297
- timeout | 2298
- local-engine | 2299
- message-processing-model | 2300
- notify | 2301
- notify-filter (Applying to the Management Target) | 2302
- notify-filter (Configuring the Profile Name) | 2303
- notify-view | 2304
- oid (SNMPv3) | 2305
- parameters | 2306
- port | 2307
- privacy-3des | 2308
- privacy-aes128 | 2309
- privacy-des | 2310
- privacy-key | 2311
- privacy-none | 2312

- privacy-password | **2313**
- read-view | **2314**
- remote-engine | **2315**
- routing-instance | **2317**
- security-level (Defining Access Privileges) | **2318**
- security-level (Generating SNMP Notifications) | **2319**
- security-model (Access Privileges) | **2320**
- security-model (Group) | **2321**
- security-model (SNMP Notifications) | **2322**
- security-name (Community String) | **2323**
- security-name (Security Group) | **2324**
- security-name (SNMP Notifications) | **2325**
- security-to-group | **2326**
- snmp-community | **2327**
- tag | **2328**
- tag-list | **2329**
- target-address | **2330**
- target-parameters | **2331**
- type | **2332**
- user | **2333**
- usm | **2334**
- v3 | **2336**
- vacm | **2340**
- write-view | **2341**

address

Syntax

```
address address;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

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

Description

Specify the SNMP target address.

Options

address—IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Address | 684

address-mask

Syntax

```
address-mask address-mask;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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 on the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Verify the source addresses for a group of target addresses.

Options

address-mask combined with the address defines a range of addresses.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Address Mask | 684

authentication-key

Syntax

```
authentication-key authentication-key;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username authentication-md5],
[edit snmp v3 usm local-engine user username authentication-sha],
[edit snmp v3 usm remote-engine engine-id user username authentication-md5],
[edit snmp v3 usm remote-engine engine-id user username authentication-sha]
```

Release Information

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

Description

Configure the key for user authentication, if you know it, instead of entering a cleartext password. The encrypted version of a password is known as a key.

Options

authentication-key—The encrypted version from the cleartext password.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MD5 Authentication | 665
Configuring SHA Authentication | 666

authentication-md5

Syntax

```
authentication-md5 {
    (authentication-key authentication-key | authentication-password authentication-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

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 MD5 as the authentication type for the SNMPv3 user.

NOTE: You can only configure one authentication type for each SNMPv3 user.

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MD5 Authentication | 665

authentication-none

Syntax

```
authentication-none;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure that there should be no authentication for the SNMPv3 user.

NOTE: You can configure only one authentication type for each SNMPv3 user.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring No Authentication | 666

authentication-password

Syntax

```
authentication-password authentication-password;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username authentication-md5],
[edit snmp v3 usm local-engine user username authentication-sha],
[edit snmp v3 usm remote-engine engine-id user username authentication-md5],
[edit snmp v3 usm remote-engine engine-id user username authentication-sha]
```

Release Information

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

Description

Configure the password for user authentication.

Options

authentication-password—Password that a user enters. The password is then converted into a key that is used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MD5 Authentication | 665
Configuring SHA Authentication | 666

authentication-sha

Syntax

```
authentication-sha {
    (authentication-key authentication-key | authentication-password authentication-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the secure hash algorithm (SHA) as the authentication type for the SNMPv3 user.

NOTE: You can configure only one authentication type for each SNMPv3 user.

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SHA Authentication | 666

community-name

Syntax

```
community-name community-name;
```

Hierarchy Level

```
[edit snmp v3 snmp-community community-index]
```

Release Information

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

Description

The community name defines an SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects.

Options

community-name—Community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose it in quotation marks (" ").

> **NOTE:** Community names must be unique. You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community *community-index*]** hierarchy levels.
>
> The community name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level is encrypted and not displayed in the command-line interface (CLI).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | 703

context (SNMPv3)

Syntax

```
context context-name;
```

Hierarchy Level

```
[edit snmp v3 snmp-community community-index]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the SNMPv3 context for access control. A context identifies a collection of information accessible for an SNMP entity.

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | 703

engine-id

Syntax

```
engine-id {
    (local engine-id-suffix | use-default-ip-address | use-mac-address);
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*. You can configure the suffix here.

> **NOTE:** SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords are based on the previous engine ID.
>
> For the engine ID, we recommend using the MAC address of the management port.

Options

local *engine-id-suffix*—Explicit setting for the engine ID suffix.

use-default-ip-address—(Does not work on Junos OS Evolved) The engine ID suffix is generated from the default IP address.

Default: use-default-ip-address

use-mac-address—(Does not work on Junos OS Evolved) The SNMP engine identifier is generated from the MAC address of the management interface on the router.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring the Local Engine ID | **701**

group (Configuring Group Name)

Syntax

```
group group-name {
   (default-context-prefix | context-prefix context-prefiix){
      security-model (any | usm | v1 | v2c) {
         security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
         }
      }
   }
}
```

Hierarchy Level

```
[edit snmp v3 vacm access]
```

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

Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The **default-context-prefix** statement, when included, adds all the contexts configured on the device to the group, whereas the **context-prefix *context-prefix*** statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series and OCX Series.) When the context prefix is specified as default (for example, **context-prefix default**), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as **logical system/routing instance**. For example, to specify routing instance ri1 in logical system ls1, include **context-prefix ls1/ri1**.

The remaining statements under this hierarchy are explained separately.

Options

group-name—SNMPv3 group name created for the SNMPv3 group.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring the Group | 671

group (Defining Access Privileges for an SNMPv3 Group)

Syntax

```
group group-name;
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name security-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Define access privileges granted to a group.

Options

group-name—Identifies a collection of SNMP security names that belong to the same access policy SNMP.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Group | 677

retry-count

Syntax

```
retry-count number;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Configure the retry count for SNMP informs.

Options

number—Maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.

Default: 3 times

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Informs | 692

timeout | 2298

timeout

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Configure the timeout period (in seconds) for SNMP informs.

Options

seconds—Number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted.

Default: 15

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SNMP Informs | 692

retry-count | 2210

local-engine

Syntax

```
local-engine {
    user username {
        authentication-md5 {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        authentication-none;
        authentication-sha {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        privacy-aes128 {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-3des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-none {
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3 usm]
```

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 local engine information for the user-based security model (USM).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

message-processing-model

Syntax

```
message-processing-model (v1 | v2c | v3);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameter-name parameters]
```

Release Information

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

Description

Configure the message processing model to be used when generating SNMP notifications.

Options

v1—SNMPv1 message process model.

v2c—SNMPv2c message process model.

v3—SNMPv3 message process model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Message Processing Model | 690

notify

Syntax

```
notify name {
   tag tag-name;
   type (trap | inform);
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

Statement introduced before Junos OS Release 7.4.
type inform option added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.

Options

name—Name assigned to the notification.

tag-name—Notifications are sent to all targets configured with this tag.

type—Notification type is **trap** or **inform**. Traps are unconfirmed notifications. Informs are confirmed notifications.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Inform Notification Type and Target Address | 693
Configuring the SNMPv3 Trap Notification | 680

notify-filter (Applying to the Management Target)

Syntax

```
notify-filter profile-name;
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the notify filter to be used by a specific set of target parameters.

Options

profile-name—Name of the notify filter to apply to notifications.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying the Trap Notification Filter | 689

notify-filter (Configuring the Profile Name)

Syntax

```
notify-filter profile-name {
    oid oid (include | exclude);
}
```

Hierarchy Level

```
[edit snmp v3]
```

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

Specify a group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.

Options

profile-name—Name assigned to the notify filter.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Notification Filter | 682
oid (SNMPv3) | 2193

notify-view

Syntax

```
notify-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
```

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

Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—Name of the view to which the SNMP user group has access.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MIB Views | **612**

Configuring the Notify View | **673**

oid (SNMPv3)

Syntax

```
oid oid <include | exclude>;
```

Hierarchy Level

```
[edit snmp v3 notify-filter profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify an object identifier (OID) used to represent a subtree of MIB objects. This OID is a prefix that the represented MIB objects have in common.

Default

include. The subtree of MIB objects represented by the specified OID is included.

Options

exclude—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

oid—Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

Required Privilege Level

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

RELATED DOCUMENTATION

SNMPv3 Overview (QFX in Standalone Mode) | **396**

Minimum SNMPv3 Configuration on a Device Running Junos OS | **657**

Configuring SNMP | **550**

Configuring the Trap Notification Filter | 682

parameters

Syntax

```
parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (none | authentication | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
}
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-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.

Description

Configure a set of target parameters for message processing and security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining and Configuring the Trap Target Parameters | 688

port

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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.

Description

Configure a UDP port number for an SNMP target.

Default

If you omit this statement, the default port is 162.

Options

port-number—Port number for the SNMP target.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Port | 685

privacy-3des

Syntax

```
privacy-3des {
   (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-aes128

Syntax

```
privacy-aes128 {
    (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-des

Syntax

```
privacy-des {
    (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

Release Information

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

Description

Configure the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-key

Syntax

```
privacy-key privacy-key;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username privacy-3des],
[edit snmp v3 usm local-engine user username privacy-aes128],
[edit snmp v3 usm local-engine user username privacy-des],
[edit snmp v3 usm remote-engine engine-id user username privacy-3des],
[edit snmp v3 usm remote-engine engine-id user username privacy-aes128],
[edit snmp v3 usm remote-engine engine-id user username privacy-des]
```

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 a privacy key for the SNMPv3 user, if you know it. The encrypted version of a password is known as a key.

Options

privacy-key—The encrypted version from the cleartext password. It is an alternative to entering a password.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-none

Syntax

```
privacy-none;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username],
[edit snmp v3 usm remote-engine engine-id user username]
```

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 that no encryption be used for the SNMPv3 user.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

privacy-password

Syntax

```
privacy-password privacy-password;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username privacy-3des],
[edit snmp v3 usm local-engine user username privacy-aes128],
[edit snmp v3 usm local-engine user username privacy-des],
[edit snmp v3 usm remote-engine engine-id user username privacy-3des],
[edit snmp v3 usm remote-engine engine-id user username privacy-aes128],
[edit snmp v3 usm remote-engine engine-id user username privacy-des]
```

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 a privacy password for the SNMPv3 user.

Options

privacy-password—Password that a user enters. The password is then converted into a key that is used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Encryption Type | 667

read-view

Syntax

```
read-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
```

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

Associate the read-only view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—The name of the view to which the SNMP user group has access.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Read View | 674

Configuring MIB Views | 612

remote-engine

Syntax

```
remote-engine engine-id {
    user username {
        authentication-md5 {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        authentication-none;
        authentication-sha {
            (authentication-key authentication-key | authentication-password authentication-password);
        }
        privacy-aes128 (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-3des {
            (privacy-key privacy-key | privacy-password privacy-password);
        }
        privacy-none {
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3 usm]
```

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.

Options

engine-id—Specify engine identifier in hexadecimal format. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring the Remote Engine and Remote User | 696

routing-instance

Syntax

```
routing-instance routing-instance-name;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-name]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify a routing instance for an SNMPv3 trap target.

Options

routing-instance-name—Name of the routing instance.

To configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (**/**) to separate the two names (for example, **test-ls/test-ri**). To configure the default routing instance on a logical system, specify the logical system name followed by **default** (for example, **test-ls/default**).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Target Address | 683

security-level (Defining Access Privileges)

Syntax

```
security-level (authentication | none | privacy) {
    notify-view view-name;
    read-view view-name;
    write-view view-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c)]
```

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

Define the security level used for access privileges.

Default

none

Options

authentication—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Level | 672

security-level (Generating SNMP Notifications)

Syntax

```
security-level (authentication | none | privacy);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security level to use when generating SNMP notifications.

Default

none

Options

authentication—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Level | 691

security-model (Access Privileges)

Syntax

```
security-model (usm | v1 | v2c);
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)]
```

Release Information

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

Description

Configure the security model for an SNMPv3 group. The security model is used to determine access privileges for the group.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 671

security-model (Group)

Syntax

```
security-model (usm | v1 | v2c) {
    security-name security-name {
        group group-name;
    }
}
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group]
```

Release Information

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

Description

Define a security model for a group.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 676

security-model (SNMP Notifications)

Syntax

```
security-model (usm | v1 | v2c);
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security model for an SNMPv3 group. The security model is used for SNMP notifications.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Model | 690

security-name (Community String)

Syntax

```
security-name security-name;
```

Hierarchy Level

```
[edit snmp v3 snmp-community community-index]
```

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

Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Options

security-name—Name that is used for messaging security and user access control.

> **NOTE:** The security name must match the configured security name at the **[edit snmp v3 target-parameters *target-parameters-name* parameters]** hierarchy level when you configure traps or informs.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Names | 705

security-name (Security Group)

Syntax

```
security-name security-name {
    group group-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
```

Release Information

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

Description

Associate a group or a community string with a configured security group.

Options

security-name—Username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Assigning Security Names to Groups | 677

security-name (SNMP Notifications)

Syntax

```
security-name security-name;
```

Hierarchy Level

```
[edit snmp v3 target-parameters target-parameters-name parameters]
```

Release Information

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

Description

Configure the security name used when generating SNMP notifications.

Options

security-name—If the SNMPv3 USM security model is used, identify the user when generating the SNMP notification. If the v1 or v2c security models are used, identify the SNMP community used when generating the notification.

> **NOTE:** The access privileges for the group associated with this security name must allow this notification to be sent.
>
> If you are using the v1 or v2 security models, the security name at the **[edit snmp v3 vacm security-to-group]** hierarchy level must match the security name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Security Name | **691**

security-to-group

Syntax

```
security-to-group {
    security-model (usm | v1 | v2c) {
        group group-name;
        security-name security-name;
    }
}
```

Hierarchy Level

```
[edit snmp v3 vacm]
```

Release Information

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

Description

Configure the group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Assigning Security Model and Security Name to a Group | 676

snmp-community

Syntax

```
snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}
```

Hierarchy Level

```
[edit snmp v3]
```

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 SNMP community.

Options

community-index—(Optional) String that identifies an SNMP community.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the SNMPv3 Community | 703

tag

Syntax

```
tag tag-name;
```

Hierarchy Level

```
[edit snmp v3 notify name],
[edit snmp v3 snmp-community community-index]
```

Release Information

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

Description

Configure a set of targets to receive traps or informs (for IPv4 packets only).

Options

tag-name—Identifies the address of managers that are allowed to use a community string.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Tag | 705

Configuring the SNMPv3 Trap Notification | 680

tag-list

Syntax

```
tag-list tag-list;
```

Hierarchy Level

```
[edit snmp v3 target-address target-address-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.

Description

Configure an SNMP tag list used to select target addresses.

Options

tag-list—Define sets of target addresses (tags). To specify more than one tag, specify the tag names as a space-separated list enclosed within double quotes.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Target Address | 685

target-address

Syntax

```
target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    retry-count number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
}
```

Hierarchy Level

```
[edit snmp v3]
```

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 address of an SNMP management application and the parameters to be used in sending notifications.

Options

target-address-name—String that identifies the target address.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Trap Target Address | 683

target-parameters

Syntax

At the **[edit snmp v3]** hierarchy level:

```
target-parameters target-parameters-name {
    profile-name;
    parameters {
        message-processing-model (v1 | v2c | V3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}
```

At the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
target-parameters target-parameters-name;
```

Hierarchy Level

```
[edit snmp v3]
[edit snmp v3 target-address target-address-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.

Description

Configure the message processing and security parameters for sending notifications to a particular management target. The target parameters are configured at the **[edit snmp v3]** hierarchy level. The remaining statements at this level are explained separately.

Then apply the target parameters configured at the **[edit snmp v3 target-parameters *target-parameters-name*]** hierarchy level to the target address configuration at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining and Configuring the Trap Target Parameters | 688
Applying Target Parameters | 686

type

Syntax

```
type (inform | trap);
```

Hierarchy Level

```
[edit snmp v3 notify name]
```

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

Description
Configure the type of SNMP notification.

Options
inform—Defines the type of notification as an inform. SNMP informs are confirmed notifications.

trap—Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.

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

RELATED DOCUMENTATION

Configuring SNMP Informs | 692
Configuring the SNMPv3 Trap Notification | 680

user

Syntax

```
user username;
```

Hierarchy Level

```
[edit snmp v3 usm local-engine],
[edit snmp v3 usm remote-engine engine-id]
```

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

Specify a user associated with an SNMPv3 group on a local or remote SNMP engine.

Options

username—SNMPv3 user-based security model (USM) username.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

usm

Syntax

```
usm {
    local-engine {
        user username {
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none {
                privacy-password privacy-password;
            }
        }
        remote-engine engine-id {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-none;
                authentication-sha {
                    authentication-password authentication-password;
                }
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-3des {
                    privacy-password privacy-password;
                }
```

```
            privacy-none {
               privacy-password privacy-password;
            }
         }
      }
   }
}
```

Hierarchy Level

```
[edit snmp v3]
```

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 user-based security model (USM) information.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating SNMPv3 Users | 662

Configuring the Remote Engine and Remote User | 696

v3

Syntax

```
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance instance;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);
            security-model (usm | v1 | v2c);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-sha {
                    authentication-password authentication-password;
```

```
            }
            authentication-none;
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-none;
        }
    }
    remote-engine engine-id {
        user username {
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-sha {
                authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none {
                privacy-password privacy-password;
            }
        }
    }
}
```

```
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix){
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c) {
            security-name security-name {
                group group-name;
            }
        }
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

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

Description

Configure SNMPv3.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Minimum SNMPv3 Configuration on a Device Running Junos OS | 657

vacm

Syntax

```
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix){
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c);
        security-name security-name {
            group group-name;
        }
    }
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

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

Description

Configure view-based access control model (VACM) information.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Defining Access Privileges for an SNMP Group | 669

write-view

Syntax

```
write-view view-name;
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) security-level  (authentication | none | privacy)]
```

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 switches.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options

view-name—Name of the view for which the SNMP user group has write permission.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring MIB Views | 612
Configuring the Write View | 674

CHAPTER 73

Configuration Statements: Uplink Failure Detection

IN THIS CHAPTER

- action (Uplink Failure Detection) | **2343**
- group (Uplink Failure Detection) | **2344**
- link-to-disable | **2345**
- link-to-monitor | **2346**
- traceoptions (Uplink Failure Detection) | **2347**
- uplink-failure-detection | **2349**

action (Uplink Failure Detection)

Syntax

```
action {
   log;
}
```

Hierarchy Level

[edit protocols **uplink-failure-detection**]

Release Information
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Define an action on uplink-failure-detection group state change.

Options

log—Generate a system log message.

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

group (Uplink Failure Detection)

Syntax

```
group  group-name {
    debounce-interval seconds;
    link-to-monitor interface-name;
    link-to-disable interface-name;
}
```

Hierarchy Level

```
[edit protocols uplink-failure-detection]
```

Release Information

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

Description

Configure a group of uplink and downlink interfaces for uplink failure detection. You can also configure the debounce interval, which is the amount of time, in seconds, that elapses before the downlink interfaces are brought up after a state change of the uplink interfaces.

Options

group-name—Name of the uplink-failure-detection group.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

link-to-disable

Syntax

```
link-to-disable interface-name;
```

Hierarchy Level

```
[edit protocols uplink-failure-detection group group-name]
```

Release Information

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

Description

Configure the downlink interfaces to be disabled when the switch detects an uplink failure. The switch can monitor a maximum of 48 downlink interfaces in a group.

Options

interface-name—Name of the downlink interface or interface range in the group. The interface can be a physical interface or a logical interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

link-to-monitor

Syntax

```
link-to-monitor interface-name;
```

Hierarchy Level

```
[edit protocols uplink-failure-detection group group-name]
```

Release Information

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

Description

Configure the uplink interfaces to be monitored for uplink failure detection. The switch can monitor a maximum of 48 uplink interfaces in a group.

An interface can be configured as link-to-monitor in multiple groups.

Options

interface-name—Name of the uplink interface or interface range in the group. The interface can be a physical interface or a logical interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

traceoptions (Uplink Failure Detection)

Syntax

```
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

[edit protocols uplink-failure-detection]

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Define tracing operations for uplink failure detection.

Default

The **traceoptions** feature is disabled by default.

Options

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.

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 (***xk*** to specify KB, ***xm*** to specify MB, or ***xg*** to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag* —Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **all**—Trace everything.
- **dcd**—Trace ufdd interaction with dcd.
- **groups**—Trace uplink-failure-detection group handling.
- **interface**—Trace interface notifcation handlers of ufdd.
- **parse**—Trace configuration parsing.

no-stamp—(Optional) Do not place a timestamp on any trace file.

no-world-readable—(Optional) Restricted file access to the user who created the file.

size *size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify gigabytes

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

admin—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

uplink-failure-detection

Syntax

```
uplink-failure-detection {
    action {
        log;
    }
    group group-name {
        debounce-interval seconds;
        link-to-monitor interface-name;
        link-to-disable interface-name;
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag);
    }
}
```

Hierarchy Level

```
[edit protocols]
```

Release Information

Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure uplink and downlink interfaces in a group to monitor uplink failures and to propagate uplink failures to the downlink interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

CHAPTER 74

Cofiguration Statements: Port Mirroring and Analyzers

IN THIS CHAPTER

- analyzer (Port Mirroring) | **2352**
- analyzer | **2354**
- bridge-domain (Analyzer) | **2356**
- disable (Forwarding Options) | **2357**
- disable-all-instances | **2358**
- ethernet-switching (Port Mirroring) | **2359**
- egress | **2360**
- egress (Analyzer) | **2361**
- ethernet-switching-options | **2362**
- family (Port Mirroring) | **2371**
- family (Port Mirroring) | **2373**
- forwarding-options | **2375**
- inet (Port Mirroring) | **2381**
- ingress (Analyzer) | **2382**
- ingress (Port Mirroring) | **2383**
- ingress (vlans) | **2384**
- input | **2385**
- input (Analyzer) | **2387**
- input (Port Mirroring) | **2389**
- instance | **2390**
- instance (Port Mirroring) | **2392**
- interface (Analyzer) | **2394**
- interface (Next-Hop Group) | **2395**
- interface (Port Mirroring) | **2396**
- interface (Port Mirroring) | **2397**
- ip-address (Port Mirroring) | **2398**
- maximum-packet-length | **2399**
- mirror-once | **2401**

- next-hop-group (Analyzer) | **2402**
- next-hop-group (Port Mirroring) | **2403**
- no-tag | **2404**
- no-tag | **2405**
- no-tag | **2406**
- no-filter-check | **2407**
- no-filter-check | **2408**
- output | **2409**
- output (Mirroring) | **2410**
- output (Port Mirroring) | **2411**
- output (Port Mirroring) | **2412**
- port-mirroring | **2414**
- rate (Forwarding Options) | **2419**
- routing-instance | **2421**
- routing-instance (Port Mirroring) | **2422**
- run-length | **2423**
- vlan (Mirroring) | **2424**
- vlan (Port Mirroring) | **2425**
- vlan (Port Mirroring) | **2426**

analyzer (Port Mirroring)

Syntax

```
analyzer {
    analyzer-name {
        input {
            egress {
                bridge-domain bridge-domain-name;
                interface (all | interface-name);
                routing-instance {
                    instance-name {
                        bridge-domain bridge-domain-name;
                    }
                }
            }
            ingress {
                bridge-domain bridge-domain-name;
                interface (all | interface-name);
                routing-instance {
                    instance-name {
                        bridge-domain bridge-domain-name;
                    }
                    vlan (vlan-id | vlan-name);
                }
                vlan (vlan-id | vlan-name);
            }
            maximum-packet-length bytes;
            rate number;
        }
        output {
            bridge-domain bridge-domain-name;
            interface interface-name;
            next-hop-group next-hop-group-name;
            routing-instance {
                instance-name {
                    bridge-domain {
                        bridge-domain-name;
                    }
                }
                vlan (vlan-id | vlan-name);
            }
            vlan (vlan-id | vlan-name);
        }
    }
```

```
}
```

Hierarchy Level

```
[edit forwarding-options]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Configure port mirroring.

Default

Port mirroring is disabled and Junos OS creates no default analyzers.

Options

analyzer-name—Name that identifies the analyzer. The name can be up to 125 characters long, must begin with a letter, and can include uppercase letters, lowercase letters, numbers, dashes, and underscores. No other special characters are allowed.

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

Understanding Port Mirroring Analyzers | **1214**

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

analyzer

Syntax

```
analyzer {
    name {
        input {
            egress {
                interface (all | interface-name);
                vlan (vlan-id | vlan-name);
            }
            ingress {
                interface (all | interface-name);
                vlan (vlan-id | vlan-name);
            }
        output {
            interface interface-name;
            ip-address ip-address;
            routing-instance
            vlan (vlan-id | vlan-name);
        }
    }
}
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options]
```

For platforms with ELS:

```
[edit forwarding-options]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.
Option **output ip-address** added in Junos OS Release 12.3 for the QFX Series for non-ELS platforms and added in 14.1X53-D10 for ELS platforms.

Description

Configure port mirroring. You can create a total of four port-mirroring configurations on the QFX Series, subject to the following limits:

- There can be no more than two configurations that mirror ingress traffic.
- There can be no more than two configurations that mirror egress traffic.

Default

Port mirroring is disabled, and Junos OS creates no default analyzers.

Options

all—Mirror all the access interfaces. Using this option does not cause the QSFP+ or management interfaces to be mirrored.

> **CAUTION:** Configuring the **all** option in a QFabric system causes all the access interfaces on all the nodes to be mirrored. Be cautious about using this option on a QFabric system.

name—Name of the analyzer. The name can include as many as 125 characters; must begin with a letter; and can include uppercase letters, lowercase letters, numbers, dashes, and underscores. No other special characters are allowed.

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

Understanding Port Mirroring and Analyzers | **1175**

Configuring Port Mirroring | **1429**

Examples: Configuring Port Mirroring for Local Analysis | **1436**

bridge-domain (Analyzer)

Syntax

```
bridge-domain bridge-domain-name;
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name input egress],
[edit forwarding-options analyzer analyzer-name input egress routing-instance instance-name],
[edit forwarding-options analyzer analyzer-name input ingress],
[edit forwarding-options analyzer analyzer-name input ingress routing-instance instance-name],
[edit forwarding-options analyzer analyzer-name output],
[edit forwarding-options analyzer analyzer-name output routing-instance instance-name]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Configure the bridge domain to monitor outgoing traffic.

Options

bridge-domain-name—Name of the bridge domain that monitors outgoing traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**

disable (Forwarding Options)

Syntax

```
disable;
```

Hierarchy Level

```
[edit forwarding-options port-mirror],
[edit forwarding-options port-mirror instance instance-name],
[edit forwarding-options sampling],
[edit forwarding-options sampling instance instance-name],
[edit forwarding-options sampling family (inet | inet6 | mpls | vpls) ],
[edit forwarding-options sampling family (inet | inet6 | mpls | vpls) output file]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement added to **port-mirror** hierarchy in Junos OS Release 9.6.

NOTE: Beginning in Junos OS Release 15.1F5 and later 15.1 releases and Junos OS Release 16.1 and later, the **disable** option has been deprecated at the **forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls)** hierarchy level on PTX3000 Series routers. When configured, the option does not take effect, so packets continue to be sampled. Instead of the **disable** option, use the **deactivate forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls)** command to prevent sampling.

Description

Disable traffic accounting, port mirroring, or sampling.

NOTE: The **disable** statement at the **[edit forwarding-options sampling]** hierarchy level disables only Routing Engine-based sampling. To disable PIC-based sampling and inline sampling, include the **disable** statement at the **[edit forwarding-options sampling instance *instance-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

Disabling Traffic Sampling

Configuring Traffic Sampling on MX, M and T Series Routers

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

disable-all-instances

Syntax

```
disable-all-instances;
```

Hierarchy Level

```
[edit forwarding-options port-mirror]
```

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Disable all port mirroring instances globally.

Usage Guidelines

See *Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers*.

Required Privilege Level

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

ethernet-switching (Port Mirroring)

Syntax

```
ethernet-switching;
output {
   interface interface-name {
   }
   no-filter-check;
   }
   vlan vlan-name {
      no-tag;
   }
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring [instance name] family]
```

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

Specify that the output interface for the port mirror will be configured as an **ethernet-switching** interface.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Port Mirroring and Analyzers | **1175**
- Configuring Port Mirroring | **1429**
- Examples: Configuring Port Mirroring for Local Analysis | **1436**

egress

Syntax

```
egress {
   interface (all | interface-name);
   }
vlan (vlan-id | vlan-name);
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name input]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name input]
```

Release Information

Statement introduced in Junos OS Release 11.2 for the QFX Series.

Description

Specify interface or VLAN for which egressing traffic is mirrored. (The **vlan** statement is not supported on all switches.)

The remaining statement is explained separately. See CLI Explorer.

> **NOTE:** If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs. If you do so, some of the mirrored packets might contain incorrect VLAN IDs.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Configuring Port Mirroring | 1429

Examples: Configuring Port Mirroring for Local Analysis | 1436

egress (Analyzer)

Syntax

```
egress {
    bridge-domain bridge-domain-name;
    interface (all | interface-name);
    routing-instance {
        instance-name {
            bridge-domain bridge-domain-name;
        }
    }
}
```

Hierarchy Level

[edit forwarding-options analyzer *analyzer-name* input]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Specify ports where traffic exiting the interface is to be mirrored in a mirroring configuration.

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

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | 1268

ethernet-switching-options

List of Syntax

EX Series on page 2362
QFX Series, QFabric, EX4600 on page 2367

EX Series

```
ethernet-switching-options {
   analyzer (Port Mirroring) {
      name {
         loss-priority priority;
         ratio number;
         input {
            ingress {
               interface (all | interface-name);
               vlan (vlan-id | vlan-name);
            }
            egress {
               interface (all | interface-name);
            }
         }
         output {
            interface interface-name;
            vlan (vlan-id | vlan-name) {
            no-tag;
            }
         }
      }
   }
   bpdu-block {
      disable-timeout timeout;
      interface (all | [interface-name]) {
         (disable | drop | shutdown);
         }
   }
   dot1q-tunneling {
      ether-type (0x8100 | 0x88a8 | 0x9100);
   }
   interfaces interface-name {
      no-mac-learning;
   }
   mac-lookup-length number-of-entries;
}
   mac-notification {
```

```
    notification-interval seconds;
}
mac-table-aging-time seconds;
nonstop-bridging;
port-error-disable {
    disable-timeout timeout;
}
redundant-trunk-group {
    group name {
        interface interface-name <primary>;
        interface interface-name;
    }
}
```

```
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ip ip-address {
            vlan  vlan-name;
            mac mac-address;
        }
        static-ipv6 ip-address {
            vlan  vlan-name;
            mac mac-address;
        }
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class class-name;
        }
        dhcp-option82 {
            circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
```

```
        vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option-37;
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag flag <disable>;
}
```

```
    unknown-unicast-forwarding {
        vlan (all | vlan-name) {
            interface interface-name;
        }
    }
    voip {
        interface (all | [interface-name | access-ports]) {
            forwarding-class forwarding-class;
            vlan vlan-name;
        }
    }
}
```

QFX Series, QFabric, EX4600

```
ethernet-switching-options {
    analyzer {
        name {
            input {
                egress {
                    interface (all | interface-name);
                }
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
            output {
                interface interface-name;
                ip-address ip-address;
                vlan (vlan-id | vlan-name);
            }
        }
    }
    bpdu-block {
        interface (all | [interface-name]);
        disable-timeout timeout;
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100)
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-table-aging-time seconds {
    }
    port-error-disable {
        disable-timeout timeout;
    }
    secure-access-port {
        dhcp-snooping-file {
            location local_pathname | remote_URL;
            timeout seconds;
            write-interval seconds;
        }
        interface (all | interface-name) {
            allowed-mac {
                mac-address-list;
            }
```

```
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action action;
        no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        dhcp-option82 {
            circuit-id {
                prefix (Circuit ID for Option 82) hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix (Remote ID for Option 82) hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
            forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        examine-fip {
            examine-vn2vn {
                beacon-period milliseconds;
            }
            fc-map fc-map-value;
        }
        mac-move-limit limit <fabric-limit limit action action;
    }
}
static {
    vlan vlan-id {
        mac mac-address next-hop interface-name;
    }
}
```

```
    storm-control {
        interface (all | interface-name) {
            bandwidth bandwidth;
            no-broadcast;
            no-multicast;
            no-unknown-unicast;
        }
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag <disable>;
    }
}
```

Hierarchy Level

```
[edit]
```

Release Information

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

Description

Configure Ethernet switching options.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Understanding How to Protect Access Ports from Common Attacks

Port Security Features

Understanding BPDU Protection for STP, RSTP, and MSTP

Understanding Redundant Trunk Links (Legacy RTG Configuration)

Understanding Storm Control

Understanding 802.1X and VoIP on EX Series Switches

Understanding Q-in-Q Tunneling and VLAN Translation

Understanding and Preventing Unknown Unicast Forwarding

Understanding MAC Notification on EX Series Switches

Understanding FIP Snooping

Understanding Nonstop Bridging on EX Series Switches

family (Port Mirroring)

List of Syntax

MX, M, T Series Routers, EX Series Switches and SRX Series Firewalls on page 2371
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 2371

MX, M, T Series Routers, EX Series Switches and SRX Series Firewalls

```
family (inet | inet6) {
    output {
        interface interface-name {
            next-hop address;
        }
        no-filter-check;
    }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
family
    ethernet-switching {
        output {
            interface interface-name {
            }
            no-filter-check;
            }
            vlan vlan-name {
                no-tag;
            }
        }
    inet
        output {
            ip-address address {
            }
            routing-instance instance-name {
                ip-address address {
            }
        }
```

Hierarchy Level

```
[edit forwarding-options port-mirroring]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T Series routers, EX Series switches and SRX Series firewalls.
Statement introduced in Junos OS Release 13.2 for the QFX Series and EX4600.

Description

Specify the type of interface that will be used to forward port mirrored packet to an analyzer device. Configure the protocol family to be sampled. Only IPv4 (**inet**) and IPv6 (**inet6**) are supported.

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

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

Understanding Port Mirroring and Analyzers | **1175**

Configuring Port Mirroring | **1429**

Examples: Configuring Port Mirroring for Local Analysis | **1436**

family (Port Mirroring)

Syntax

```
family (ccc | inet | inet6 | vpls) {
   output {
      interface interface-name {
         next-hop address;
      }
      next-hop-group group-name{
         group-type inet6;
         interface interface-name {
            next-hop ipv6-address;
         }
         next-hop-subgroup group-name{
            interface interface-name {
               next-hop ipv6-address;
            }
         }
      }
      no-filter-check;
      server-profile server-profile-name;
   }
}
```

Hierarchy Level

[edit **forwarding-options port-mirroring**],
[edit **forwarding-options port-mirroring instance** *instance-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
vpls and **ccc** options introduced in Junos OS Release 9.3 for MX Series routers only.
vpls support extended to M7i, M10i, M120, and M320 routers in Junos OS Release 9.5.
ccc option introduced in Junos OS Release 9.6 for M120 and M320 routers only.
Statement introduced in Junos OS Release 12.1 for PTX Series Packet Transport Switches.
ccc option introduced in Junos OS Release 12.3R2 for EX Series switches.
next-hop-group option for **family inet6** introduced in Junos OS Release 14.2 for MX Series routers only.

Description

Configure the address type family to sample for port mirroring.

Options

ccc—Sample Layer 2 VPN traffic.

inet—Sample IPv4 traffic.

inet6—Sample IPv6 traffic.

vpls—Sample VPLS traffic.

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 Port Mirroring

Configuring Active Flow Monitoring on PTX Series Packet Transport Routers

forwarding-options

Syntax

```
forwarding-options {
    dhcp-security {
        arp-inspection;
        group group-name {
            interface interface-name {
                static-ip ip-address {
                    mac mac-address;
                }
            }
            overrides {
                no-option82;
                (trusted | untrusted);
            }
        }
        ip-source-guard;
        no-dhcp-snooping;
        option-82 {
            circuit-id {
                prefix {
                    host-name;
                    logical-system-name;
                    routing-instance-name;
                }
                use-interface-description (device | logical);
                use-vlan-id;
            }
            remote-id {
                host-name hostname;
                use-interface-description (device | logical);
                use-string string;
            }
            vendor-id {
                use-string string;
            }
        }
    }
    filter (VLANs) {
        input filter-name;
        output filter-name;
    }
    flood {
```

```
    input filter-name;
  }
```

Chassis: EX4600 and QFX Series

```
forwarding options profile-name {
  num-65-127-prefix number;
}
```

Chassis: EX4600 and QFX Series

```
forwarding-options lpm-profile {
  prefix-65-127-disable;
  unicast-in-lpm;
}
```

Chassis: EX4600 and QFX Series

```
forwarding-options custom-profile {
  l2-entries | l3-entries | lpm-entries {
    num-banks number;
  }
}
```

Hierarchy Level

```
[edit],
[edit bridge-domains bridge-domain-name],
[edit vlans vlan-name]
```

```
[edit chassis (QFX Series)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Hierarchy level **[edit vlans *vlan-name*]** introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Hierarchy level **[edit bridge-domains *bridge-domain-name*]** introduced in Junos OS Release 14.1 for MX Series routers.
custom-profile option introduced in Junos OS Release 15.1x53-D30 for QFX5200 Series switches only.

Description

Configure a unified forwarding table profile to allocate the amount of memory available for the following:

- MAC addresses.
- Layer 3 host entries.
- Longest prefix match table entries.

This feature enables you to select a profile that optimizes the amount of memory available for various types of forwarding-table entries based on the needs of your network. For example, for a switch that handles a great deal of Layer 2 traffic, such as a virtualized network with many servers and virtualized machines, you would choose the **l2-profile-one**, which allocates the highest amount of memory to MAC addresses.

You configure the memory allocation for LPM table entries differently, depending on whether you using Junos OS Release 13.2X51-D10 or Junos OS Release 13.2X51-D15 and later. For more information about configuring memory allocation for LPM table entries, see *Configuring the Unified Forwarding Table on Switches*.

The **num-65-127-prefix *number*** statement is not supported on the **custom-profile** and the **lpm-profile**. The **prefix-65-127-disable** and **unicast-in-lpm** statements are supported only on the **lpm-profile**.

When you commit a configuration with a forwarding table profile change, in most cases the Packet Forwarding Engine restarts automatically to apply the new parameters, which brings the data interfaces down and then up again.

However, starting with Junos OS Releases 14.1X53-D40, 15.1R5, and 16.1R3, for a Virtual Chassis or Virtual Chassis Fabric (VCF) comprised of EX4600 or QFX5100 switches, the Packet Forwarding Engine in member switches does not automatically restart upon configuring and committing a unified forwarding table profile change. This behavior avoids having Virtual Chassis or VCF instability and a prolonged convergence period if a profile change is propagated to member switches and multiple Packet Forwarding Engines all restart at the same time. In this environment, instead of automatically restarting when you initially commit a profile configuration change, the message **Reboot required for configuration to take effect** is displayed at the master switch CLI prompt, notifying you that the profile change does not take effect until the next time you restart the Virtual Chassis or VCF. The profile configuration change is propagated to member switches that support this feature, and a reminder that a reboot is required to apply this pending configuration change appears in the system log of the master switch and applicable member switches. You then enable the profile change subsequently during a planned downtime period using the **request system reboot** command, which quickly establishes a stable Virtual Chassis or VCF with the new configuration.

NOTE: You should plan to make unified forwarding table profile changes only when you are ready to perform a Virtual Chassis or VCF system reboot *immediately* after committing the configuration update. Otherwise, in the intervening period between committing the configuration change and rebooting the Virtual Chassis or VCF, the system can become inconsistent if a member experiences a problem and restarts. In that case, the new configuration takes effect on the member that was restarted, while the change is not yet activated on all the other members.

The remaining statements are explained separately. See CLI Explorer.

Options

profile-name—name of the profile to use for memory allocation in the unified forwarding table.

Table 208 on page 2379 lists the profiles you can choose that have set values and the associated values for each type of entry.

On QFX5200 Series switches only, you can also select **custom-profile**. This profile enables you to allocate from one to four banks of shared hash memory to a specific type of forwarding-table entry. Each shared hash memory bank can store a maximum of the equivalent of 32,000 IPv4 unicast addresses.

Table 208: Unified Forwarding Table Profiles

Profile Name	MAC Table	Host Table (unicast and multicast addresses)					
	MAC Addresses	IPv4 unicast	IPv6 unicast	IPv4 (*, G)	IPv4 (S, G)	IPv6 (*, G)	IPv6 (S, G)
l2-profile-one	288K	16K	8K	8K	8K	4K	4K
l2-profile-two	224K	80K	40K	40K	40K	20K	20K
l2-profile-three (default)	160K	144K	72K	72K	72K	36K	36K
l3-profile	96K	208K	104K	104K	104K	52K	52K
lpm-profile*	32K	16K	8K	8K	8K	4K	4K

* This profile supports only IPv4 in Junos OS Release13.2X51-D10. Starting in Junos OS Relase13.2X51-D15, the **lpm-profile** supports IPv4 and IPv6 entries.

NOTE: If the host stores the maximum number of entries for any given type, the entire table is full and is unable to accommodate *any* entries of any other type. For information about valid combinations of table entries see *Understanding the Unified Forwarding Table*.

l2-entries | l3-entries | lpm-entries—(**custom-profile only**) Select a type of forwarding-table entry—Layer 2, Layer 3, or LPM—to allocate a specific number of shared memory banks. You configure the amount of memory to allocate for each type of entry separately.

num-banks *number*—(**custom-profile only**) Specify the number of shared memory banks to allocate for a specific type of forwarding-table entry. Each shared memory bank stores the equivalent of 32,000 IPv4 unicast addresses.

Range: 0 through 4.

NOTE: There are four shared memory banks, which can be allocated flexibly among the three types of forwarding-table entries. To allocate no shared memory for a particular entry type, specify the number **0**. When you commit the configuration, the system issues a commit check to ensure that you have not configured more than four memory banks. You do not have to configure all four shared memory banks. By default, each entry type is allocated the equivalent of 32,000 IPv4 unicast addresses in shared memory.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- *Understanding the Unified Forwarding Table*
- *Example: Configuring a Unified Forwarding Table Custom Profile*
- *Configuring Traffic Forwarding and Monitoring*

inet (Port Mirroring)

Syntax

```
inet {
output {
   ip-addressaddress {
   }
   routing-instance instance-name {
      ip-address address {
   }
}
```

Hierarchy Level

[edit forwarding-options port-mirroring [instance *name*] family]

Release Information

Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify that the output interface will be of type **inet**. Use this statement so that you can send the mirrored packets to the IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.)

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

Required Privilege Level

routing—To view this statement in the configuration.

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

ingress (Analyzer)

Syntax

```
ingress {
    bridge-domain bridge-domain-name;
    interface (all | interface-name);
    routing-instance {
        instance-name {
            bridge-domain bridge-domain-name;
        }
        vlan (vlan-id | vlan-name);
    }
    vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

[edit forwarding-options analyzer *analyzer-name* input]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Configure ports, routing instances, VLANs, or bridge domains for which the entering traffic is mirrored as part of a mirroring configuration.

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

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | 1268

ingress (Port Mirroring)

Syntax

```
ingress {
    interface (all | interface-name);
    vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name input]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name input]
```

Release Information

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

Description

Specify the interfaces or VLANs for which incoming traffic is mirrored as part of a port mirroring configuration.

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

- Understanding Port Mirroring and Analyzers | 1175
- Configuring Port Mirroring | 1429
- Examples: Configuring Port Mirroring for Local Analysis | 1436

ingress (vlans)

Syntax

```
ingress;
```

Hierarchy Level

```
[edit vlans vlan-name vlan-id number interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description

Specify that the member interface of the VLAN allows only ingress traffic.

Required Privilege Level

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

input

Syntax

```
input {
    ingress {
        interface (all | interface-name);
        vlan (vlan-id | vlan-name);
    }
    egress {
        interface (all | interface-name);
    }
}
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name]
```

Release Information

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

Description

Define the traffic to be mirrored. The definition can be a combination of traffic entering or exiting specific ports or VLANs.

The remaining statements are explained separately. See CLI Explorer.

Default

No default.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Configuring Port Mirroring | 1429

Examples: Configuring Port Mirroring for Local Analysis | 1436

input (Analyzer)

Syntax

```
input {
    egress {
        bridge-domain bridge-domain-name;
        interface (all | interface-name);
        routing-instance {
            instance-name {
                bridge-domain bridge-domain-name;
            }
        }
    }
    ingress {
        bridge-domain bridge-domain-name;
        interface (all | interface-name);
        routing-instance {
            instance-name {
                bridge-domain bridge-domain-name;
            }
            vlan (vlan-id | vlan-name);
        }
        vlan (vlan-id | vlan-name);
    }
    maximum-packet-length bytes;
    rate number;
}
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Define the traffic to be mirrored in a mirroring configuration—the definition can be a combination of:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN
- Packets entering or exiting a bridge domain

The remaining statements are explained separately. See CLI Explorer.

Native analyzer sessions (that is, the **[edit forwarding-options analyzer analyzer-name input]** hierarchy level for MX Series routers) can be configured without specifying input parameters, which would mean that the instance uses default input values: rate = 1 and maximum-packet-length = 0.

Default

No default.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**
- Understanding Port Mirroring Analyzers | **1214**

input (Port Mirroring)

Syntax

```
input {
    maximum-packet-length bytes;
    rate number;
    run-length number;
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring],
[edit forwarding-options port-mirroring instance instance-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
maximum-packet-length option introduced in Junos OS Release 9.6 for M120 and M320 routers only.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

Description

Configure input packet properties for port mirroring.

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 Port Mirroring

instance

Syntax

```
instance {
    instance-name {
        input {
            maximum-packet-length bytes;
            rate number;
            run-length number;
        }
        family (ccc| inet | inet6 | mpls | vpls) {
            output {
                interface interface-name {
                    next-hop address;
                }
                no-filter-check;
                server-profile server-profile-name;
            }
        }
    }
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring],
[edit routing-instances routing-instance-name forwarding-options port-mirroring]
```

Release Information

Statement introduced in Junos OS Release 9.3 (MX Series routers only).
Support extended to M120 and M320 routers in Junos OS Release 9.5.
maximum-packet-length and **ccc** options introduced in Junos OS Release 9.6 for M120 and M320 routers only.
server-profile option introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers only.

Description

Configure a port-mirroring instance.

Options

port-mirroring-instance-name—Name of the port-mirroring instance.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Mirroring

Configuring Active Flow Monitoring on PTX Series Packet Transport Routers

instance (Port Mirroring)

List of Syntax

Syntax: MX, M and T Series Routers and SRX Series Firewalls on page 2392
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 2392

Syntax: MX, M and T Series Routers and SRX Series Firewalls

```
instance instance-name {
    disable;
    input {
        rate number;
        maximum-packet-length bytes
    }
    family (any | inet | inet6 | vpls) {
        output {
            (next-hop-group group-name | interface interface-name);
        }
    }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
instance instance-name{
    family
        ethernet-switching {
            output {
                interface interface-name {
                }
                no-filter-check;
                }
                vlan vlan-name {
                    no-tag;
                }
            }
        inet
            output {
                ip-address address {
                }
                routing-instance instance-name {
                    ip-address address {
                }
            }
        }
```

```
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring]
```

Release Information

Statement introduced in Junos OS Release 9.6 for MX, M and T Series routers and SRX Series firewalls.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

Specify a port-mirroring configuration (instance). You do not specify an input for this instance. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This is useful for controlling which types of traffic should be mirrored.

The remaining statements are explained separately. See CLI Explorer.

Usage Guidelines

See *Configuring Sampling Instance on MX, M and T Series Routers or QFX Series Switches*.

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

- Understanding Port Mirroring and Analyzers | **1175**
- Configuring Port Mirroring | **1429**
- Examples: Configuring Port Mirroring for Local Analysis | **1436**
- Example: Mirroring Employee Web Traffic with a Firewall Filter | **1439**

interface (Analyzer)

Syntax

```
interface (all | interface-name);
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name input egress],
[edit forwarding-options analyzer analyzer-name input ingress],
[edit forwarding-options analyzer analyzer-name output]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Configure the interfaces for which traffic is mirrored.

Options

all—Apply mirroring to all interfaces on the network device. Mirroring a high volume of traffic can be performance intensive for the device. Therefore, you should generally select specific input interfaces in preference to using the **all** keyword, or use the **all** keyword in combination with setting a ratio for statistical sampling. The **all** keyword is not available for the **[edit forwarding-options analyzer *analyzer-name* output]** hierarchy level.

interface-name—Apply mirroring to the specified interface only.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | **1240**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

Understanding Port Mirroring Analyzers | **1214**

interface (Next-Hop Group)

Syntax

```
interface interface-name {
    next-hop address;
}
```

Hierarchy Level

```
[edit forwarding-options next-hop-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the output interface for sending copies of packets elsewhere to be analyzed.

The commit operation fails when a next-hop group has only one interface configured. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.

Options

interface-name—Name of the 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

Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring

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, ACX, 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 (Port Mirroring)

Syntax

```
interface (all | interface-name);
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name input (egress | ingress)],
[edit ethernet-switching-options analyzer name output]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name input (egress | ingress)]
[edit forwarding-options analyzer name output]
[edit forwarding-options port-mirroring [instance name] family ethernet-switching output]
```

Release Information

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

Description

Specify the interfaces for which ingressing traffic is mirrored. Specify the interface that mirrored traffic should be copied to (the output interface).

Options

all—Apply port mirroring to all interfaces on the switch (except the output interface). Mirroring a high volume of traffic can cause performance issues, so you should generally select specific input interfaces.

CAUTION: Configuring **all** in a QFabric system causes all the access interfaces on all the nodes to be mirrored. Be cautious about using this option on a QFabric system.

interface-name—Apply port mirroring to the specified interface only.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175
Configuring Port Mirroring | 1429
Examples: Configuring Port Mirroring for Local Analysis | 1436

ip-address (Port Mirroring)

Syntax

```
ip-address ip-address;
```

Hierarchy Level

```
[edit forwarding-options] analyzer name output]
[edit forwarding-options port-mirroring [instance name] family ethernet-switching output interface name]
```

Release Information

Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the IP address to which traffic should be mirrored (the IP address of the analyzer system). The device can be on a remote network. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) This statement is not supported on QFabric systems.

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

Required Privilege Level

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

maximum-packet-length

Syntax

```
maximum-packet-length bytes;
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name input],
[edit forwarding-options port-mirroring input],
[edit forwarding-options port-mirroring instance instance-name input],
[edit forwarding-options sampling input],
[edit forwarding-options sampling instance instance-name input]
```

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport routers. For PTX Series routers with third-generation FPCs installed, **maximum-packet-length** is not supported at the **[edit forwarding-options sampling input]** and **[edit forwarding-options sampling instance *instance-name* input]** hierarchy levels.
For MX Series routers except the MX 80, support at the **[edit forwarding-options analyzer analyzer-name input]** hierarchy level was introduced in Junos OS Release 14.1
Statement introduced in Junos OS Release 17.4R1 for QFX10008 and QFX10016 switches.

Description

Set the maximum packet length to be used for port mirroring or traffic sampling. Packets longer than the maximum are truncated. This statement cannot be used with inline flow monitoring (**[edit forwarding-options sampling instance *instance-name* family (inet | inet6) output inline-jflow]** .

> **NOTE:** For MX Series routers with Modular Port Interface Concentrators (MPCs), when **maximum-packet-length** (clip length) is configured for port-mirrored packets and the mirror-destination interface is a next-hop-group, the clip length is effective only for the first member interface of the next-hop-group. The mirrored packet copy sent to the rest of the interfaces is not clipped.
>
> In addition, native analyzer sessions (that is, the **[edit forwarding-options analyzer analyzer-name input]** hierarchy level for MX Series routers) can be configured without specifying input parameters. As such, these instances use the following input values by default: rate = 1, and maximum-packet-length = 0.

Options

bytes—Maximum length (in bytes) of the mirrored packet or the sampled packet.

Set the maximum-packet-length value to zero to disable truncation; that is, to mirror or sample the entire packet. Otherwise, Juniper recommends that you configure the packet length to be equal to, or greater than, the IP header length. For IPv4, set the maximum length to at least 20, and for IPv6, set the maximum length to at least 40.

Range: 0 through 9216. For MX Series routers with MPCs, and for EX9200 switches, the range is 1 through 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

Configuring Port Mirroring

Configuring Traffic Sampling on MX, M and T Series Routers

mirror-once

Syntax

```
mirror-once;
```

Hierarchy Level

```
[edit forwarding-options port-mirroring]
```

Release Information

Statement introduced in Junos OS Release 9.3 (MX Series routers only).
Support extended to M120 routers in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.

Description

Configure the router to mirror packets only once. This feature is useful if you configure port mirroring on both ingress and egress interfaces, which could result in the same packet being mirrored twice.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Mirroring

next-hop-group (Analyzer)

Syntax

```
next-hop-group next-hop-group-name;
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name ouput]
```

Release Information

Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Configure next-hop group through which the port-mirrored traffic is sent.

Options

next-hop-group-name—Name of the next-hop group through which the port-mirrored traffic is sent.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches | **1258**

next-hop-group (Port Mirroring)

Syntax

```
next-hop-group group-name;
```

Hierarchy Level

```
[edit forwarding-options port-mirroring family (inet | vpls) output],
[edit forwarding-options port-mirroring instance instance-name family (inet | vpls) output]
```

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Specify the next-hop address for sending copies of packets to an analyzer. This configuration enables multipacket port mirroring on MX Series routers and EX Series switches without the use of a Tunnel PIC.

The commit operation fails when a next-hop group has only one interface configured. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.

Options

group-name—Name of next-hop group.

Required Privilege Level

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

RELATED DOCUMENTATION

Port Mirroring with Next-Hop Groups

no-tag

Syntax

```
no-tag;
```

Hierarchy Level

```
[edit ethernet-switching-options analyzer name output vlan (vlan-id | vlan-name)]
[edit forwarding-options port-mirroring family ethernet-switching output vlan (vlan-name | vlan-id) ]
[edit forwarding-options port-mirroring instance instance-name family ethernet-switching output vlan (vlan-name
    | vlan-id)]
```

Release Information

Statement introduced in Junos OS Release 11.3 for EX Series switches.
Hierarchy **[edit forwarding-options port-mirroring family ethernet-switching output vlan]** introduced in Junos OS Release 13.2.
Hierarchy **[edit forwarding-options port-mirroring instance instance-name family ethernet-switching output vlan]** introduced in Junos OS Release 13.2.

Description

Specify that remote port-mirroring packets are not tagged.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches

no-tag

Syntax

```
no-tag;
```

Hierarchy Level

[edit **forwarding-options analyzer** *name* **output vlan**]
[edit **forwarding-options** port-mirroring [instance *name*] family ethernet-switching **output vlan**]

Release Information
Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches.

Description
Specify that remote mirrored packets are not tagged with the tag of the output (analyzer) VLAN.

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

RELATED DOCUMENTATION

Example: Configuring Port Mirroring for Remote Analysis | **1450**

no-tag

Syntax

```
no-tag;
```

Hierarchy Level

[edit [edit forwarding-options analyzer] Configuration Statement Hierarchy *analyzer-name* output vlan (*vlan-id* | *vlan-name*)]

Release Information

Statement introduced in Junos OS Release 11.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description

Specify that remote mirroring packets are not tagged.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches | **1286**

no-filter-check

Syntax

```
no-filter-check;
```

Hierarchy Level

```
[edit forwarding-options port-mirroring family (inet | inet6) output]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Disable filter checking on the port-mirroring interface.

This statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it.

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

RELATED DOCUMENTATION

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

no-filter-check

Syntax

```
no-filter-check;
```

Hierarchy Level

[edit **forwarding-options port-mirroring output**],
[edit **forwarding-options port-mirroring family** (inet | inet6 | ccc | vpls) **output**]

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
Disable filter checking on the port-mirroring interface.

This statement is required when you send port-mirrored traffic to a Tunnel Services PIC that has a filter applied to it.

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

RELATED DOCUMENTATION

Configuring Port Mirroring

output

Syntax

```
output {
   interface interface-name;
   ip-address ip-address;
   vlan (vlan-id | vlan-name);
   routing-instance instance-name {
      ip-address address {
}
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name]
[edit forwarding-options port-mirroring [instance name] family ethernet-switching ]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the destination for mirrored traffic, either an interface on the switch (for local monitoring) or a VLAN (for remote monitoring).

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.

output (Mirroring)

Syntax

```
output {
    bridge-domain bridge-domain-name;
    interface interface-name;
    next-hop-group next-hop-group-name;
    routing-instance {
        instance-name {
            bridge-domain {
                bridge-domain-name;
            }
        }
        vlan (vlan-id | vlan-name);
    }
    vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

Configure the destination for mirrored traffic, either an interface on the network device for local monitoring, or a VLAN or bridge domain, for remote monitoring.

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

Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use | 1240

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | 1245

output (Port Mirroring)

Syntax

```
output {
    interface interface-name {
        next-hop address;
    }
    no-filter-check;
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring family (inet | inet6)]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure output interfaces and flow 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 Port Mirroring on M, T MX, ACX, and PTX Series Routers

output (Port Mirroring)

Syntax

```
output {
    interface interface-name {
        next-hop address;
    }
    next-hop-group group-name{
        group-type inet6;
        interface interface-name {
            next-hop ipv6-address;
        }
        next-hop-subgroup group-name{
            interface interface-name {
                next-hop ipv6-address;
            }
        }
    }
    no-filter-check;
    server-profile server-profile-name;
}
```

Hierarchy Level

```
[edit forwarding-options port-mirroring family (ccc | inet | inet6 | mpls | vpls)],
[edit forwarding-options port-mirroring instance instance-name family (ccc | inet | inet6 | mpls | vpls)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
vpls option introduced in Junos OS Release 9.3 for MX Series routers only; support extended to M7i, M10i, M120, and M320 routers in Junos OS Release 9.5.
ccc option introduced in Junos OS Release 9.6 for M120 and M320 routers only.
server-profile option introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers only.
next-hop-group option introduced for **family inet6** in Junos OS Release 14.2 for MX Series routers only.

Description

Configure the port mirroring destination 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 Port Mirroring

Configuring Active Flow Monitoring on PTX Series Packet Transport Routers

port-mirroring

List of Syntax

Syntax: MX Series and PTX Series Routers, M120 and M320 on page 2414
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 2416
Syntax: OCX1100 on page 2417

Syntax: MX Series and PTX Series Routers, M120 and M320

```
port-mirroring {
    input {
        maximum-packet-length bytes;
        rate number;
        run-length number;
    }
    family (ccc | inet | inet6 | vpls) {
        output {
            interface interface-name {
                next-hop address;
            }
            next-hop-group group-name{
                group-type inet6;
                interface interface-name {
                    next-hop ipv6-address;
                }
                next-hop-subgroup group-name{
                    interface interface-name {
                        next-hop ipv6-address;
                    }
                }
            }
            no-filter-check;
        }
    }
    instance {
        instance-name {
            input {
                maximum-packet-length bytes;
                rate number;
                run-length number;
            }
            family (ccc | inet | inet6 | vpls) {
                output {
                    interface interface-name {
                        next-hop address;
```

```
                }
                no-filter-check;
                server-profile server-profile-name;
            }
        }
    }
    mirror-once;
    traceoptions {
        file filename <files number> <size bytes> <world-readable | no-world-readable>;
    }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
port-mirroring {
    family {
        ethernet-switching
            output {
                interface interface-name {
                }
                no-filter-check;
                }
                vlan vlan-name {
                    no-tag;
                }
            }
        inet
            output {
                ip-address address {
                }
                routing-instance instance-name {
                    ip-address address {
                }
            }
    }
    instance instance-name {
        family
            ethernet-switching {
                output {
                    interface interface-name {
                    }
                    no-filter-check;
                    }
                    vlan vlan-name {
                        no-tag;
                    }
                }
            inet
                output {
                    ip-address address {
                    }
                    routing-instance instance-name {
                        ip-address address {
                    }
                }
            }
        }
```

```
    }
}
```

Syntax: OCX1100

```
port-mirroring {
    family {
        inet
            output {
                ip-address address {
                }
                routing-instance instance-name {
                    ip-address address {
                }
            }
    }
    instance instance-name {
        family
            inet
                output {
                    ip-address address {
                    }
                    routing-instance instance-name {
                        ip-address address {
                    }
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit forwarding-options]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX Series and PTX Series routers, M120 and M320.
family vpls statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M7i, M10, M120, and M320 routers in Junos OS Release 9.5.
instance *port-mirroring-instance-name* statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 and M320 routers in Junos OS Release 9.5.
mirror-once statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 routers in Junos OS Release 9.5.
family ccc statement introduced in Junos OS Release 9.6 (M120 and M320 routers only).
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
family inet6 and **next-hop-group** statements introduced in Junos OS Release 14.2 (MX Series routers only).
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

Create a port-mirroring configuration. Specify the address family, rate, run length, interface, and next-hop address for sending copies of packets to an analyzer.

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

Configuring Port Mirroring

Configuring Port Mirroring | **1429**

Configuring Port Mirroring

Configuring Active Flow Monitoring on PTX Series Packet Transport Routers

Understanding Port Mirroring and Analyzers | **1175**

Understanding Port Mirroring | **1183**

Examples: Configuring Port Mirroring for Local Analysis | **1436**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1439**

Example: Mirroring Employee Web Traffic with a Firewall Filter | **1351**

rate (Forwarding Options)

Syntax

```
rate number;
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name input],
[edit forwarding-options port-mirroring family (inet | inet6) input],
[edit forwarding-options port-mirroring input],
[edit forwarding-options sampling input],
[edit forwarding-options sampling instance instance-name input]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport routers.
Support at the **[edit forwarding-options analyzer analyzer-name input]** hierarchy level for MX Series routers introduced in Junos OS Release 14.1.
Statement introduced in Junos OS Release 17.2R1 for QFX10002 switches.
Statement introduced in Junos OS Release 17.4R1 for QFX10008 and QFX10016 switches.

Description

Set the ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.

Native analyzer sessions (that is, the **[edit forwarding-options analyzer analyzer-name input]** hierarchy level for MX Series routers) can be configured without specifying input parameters, which means that the instance uses default input values: rate = 1 and maximum-packet-length = 0.

> **NOTE:** The recommended sampling rate for the MX150 is 1000 or greater. If you configure less than 1000, a warning is issued.

Options

number—Denominator of the ratio.

Range: 1 through 16000000(16M)

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Mirroring

Configuring Traffic Sampling

routing-instance

Syntax

```
routing-instance {
    instance-name {
        bridge-domain bridge-domain-name;
    }
    vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

```
[edit forwarding-options analyzer analyzer-name input egress],
[edit forwarding-options analyzer analyzer-name input ingress],
[edit forwarding-options analyzer analyzer-name output]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Configure routing instance.

Options

instance-name—Name of the routing instance.

Required Privilege Level

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

RELATED DOCUMENTATION

routing-instance (Port Mirroring)

Syntax

```
routing-instance instance-name;
```

Hierarchy Level

```
[edit forwarding-options] analyzer name output]
[edit forwarding-options port-mirroring [instance name] family inet output interface name]
```

Release Information

Statement introduced in Junos OS Release 12.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure a port mirroring instance. You do not specify an input for this instance. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This instance type is useful for controlling which types of traffic should be mirrored.

Required Privilege Level

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

run-length

Syntax

```
run-length number;
```

Hierarchy Level

```
[edit forwarding-options port-mirroring input],
[edit forwarding-options port-mirroring instance port-mirroring-instance-name input],
[edit forwarding-options port-mirroring family (inet|inet6) input],
[edit forwarding-options sampling input],
[edit forwarding-options sampling instance instance-name input]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport routers.
Statement introduced in Junos OS Release 17.2R1 for QFX10002 switches.
Statement introduced in Junos OS Release 17.4R1 for QFX10008 and QFX10016 switches.

Description

Set the number of samples following the initial trigger event. The configuration enables you to sample packets following those already being sampled.

> **NOTE:** The **run-length** statement is not supported when you configure inline flow monitoring (by including the **inline-jflow** statement at the **[edit forwarding-options sampling instance *instance-name* family (inet | inet6) output]** hierarchy level).

Options

number—Number of samples.

Range: 0 through 20

Default: 0

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Forwarding Table Filters

Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers

Configuring Traffic Sampling on MX, M and T Series Routers

vlan (Mirroring)

Syntax

vlan (*vlan-id* | *vlan-name*);

Hierarchy Level

[edit forwarding-options analyzer *analyzer-name* input ingress],
[edit forwarding-options analyzer *analyzer-name* input ingress routing-instance *instance-name*],
[edit forwarding-options analyzer *analyzer-name* output],
[edit forwarding-options analyzer *analyzer-name* output routing-instance *instance-name*]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 (ELS).

Description

Configure mirrored traffic to be sent to a VLAN for remote monitoring.

Options

vlan-id—Numeric VLAN identifier.

vlan-name—Name of the VLAN.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches | **1268**

Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use | **1245**

vlan (Port Mirroring)

Syntax

```
vlan (vlan-name | vlan-ID);
```

Hierarchy Level

```
[edit forwarding-options port-mirroring family ethernet-switching output]
[edit forwarding-options port-mirroring instance instance-name family ethernet-switching output]
```

Release Information

Statement introduced in Junos OS Release 13.2.

Description

Specify the VLAN name or ID for sending copies of packets to an analyzer. This configuration enables remote VLAN port mirroring on EX Series switches.

Options

vlan-name—Name of remote mirroring VLAN.

vlan-ID—ID of the remote mirroring VLAN.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Layer 2 Port Mirroring to Remote VLAN | **1420**

Layer 2 Port Mirroring to Remote Destination by Using Destination as VLAN | **1417**

vlan (Port Mirroring)

Syntax

```
vlan (vlan-id | vlan-name) {
    no-tag;
```

Hierarchy Level

For platforms without ELS:

```
[edit ethernet-switching-options analyzer name input ingress],
[edit ethernet-switching-options analyzer name output]
```

For platforms with ELS:

```
[edit forwarding-options analyzer name input (egress | ingress)]
[edit forwarding-options analyzer name output]
[edit forwarding-options port-mirroring [instance name] family ethernet-switching output]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option**output vlan** added in Junos OS Release 12.1 for the QFX Series.
Option**no-tag** added in Junos OS Release 15.1X53-D10 for QFX10000 switches.

Description

When used in an **input** statement, specifies that traffic entering or exiting a VLAN should be mirrored. (You can include this statement in an **ingress** statement or **egress** statement within the **input** statement. It is not supported in an **egress** statement on all switches) When used in an **output** statement, specifies that mirrored traffic to be sent to a VLAN for remote monitoring.

On some switches, only one interface can be a member of the output (analyzer) VLAN. This limitation does not apply on the QFX10000 switch if traffic is mirrored on ingress. In this case, multiple QFX10000 interfaces can belong to the output VLAN, and traffic is mirrored to all of those interfaces. If traffic is mirrored on egress on a QFX10000 switch, only one interface can be a member of the analyzer VLAN.

Options

vlan-id—Numeric VLAN identifer.

vlan-name—Name of the VLAN.

no-tag—Specifies that remote mirrored packets are not tagged with the tag of the output (analyzer) VLAN.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Port Mirroring and Analyzers | 1175

Configuring Port Mirroring | 1429

Examples: Configuring Port Mirroring for Local Analysis | 1436

CHAPTER 75

Configuration Statements: TWAMP

IN THIS CHAPTER

- twamp-server | 2429
- twamp-client | 2432

twamp-server

Syntax

```
twamp {
    server {
        authentication-mode mode;
        client-list list-name {
            address address;
        }
        max-connection-duration hours;
        maximum-connections count;
        maximum-connections-per-client count;
        maximum-sessions count;
        maximum-sessions-per-connection count;
        port number;
        routing-instance-list {
            instance-name {
                port number;
            }
        }
        server-inactivity-timeout minutes;
    }
}
```

Hierarchy Level

```
[edit services rpm twamp server]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Defines the Two-Way Active Measurement Protocol (TWAMP) server configurations. This configuration describes a TWAMP server on the router that enables a TWAMP client to connect to the server using any media interface IP address. In such scenarios, the router functions as a TWAMP server and timestamping is performed in the ukernel of the media-facing Flexible PIC Concentrator (FPC).

Options

server—TWAMP server configuration.

authentication-mode—Set of authentication modes that the server can accept.

Default: none

max-connection-duration—Maximum time a connection can exist between the client and the server.

Default: 24

Range: 0-120

maximum-sessions—Maximum number of test sessions for the server.

Default: 64

Range: 1-2048

maximum-sessions-per-connection—Maximum number of test sessions per client connection.

Default: 64

Range: 1-1024

maximum-connections—Maximum number of connections for the server.

Default: 64

Range: 1-1000

maximum-connections-per-client—Maximum number of server connections per client.

Default: 64

Range: 1-500

port—TWAMP server listening port used by the routing instance.

Default: 862

Range: 1-65535

client-list—List of allowed control client hosts that can connect to this server. Each item in the list is a Classless Interdomain Routing (CIDR) address (ip address1/mask1) that represents the network of allowed hosts.

routing-instance-list— List of allowed routing instances (a maximum of 31 characters). It configures the TWAMP servers on specific routing instances, instead of associating the TWAMP server at the system-level to apply to all routing instances configured on a router. The default routing instance is Internet routing table **inet.0**. If you do not specify a routing instance then the TWAMP probe applies to all routing instances. Up to 100 routing instances can be configured for a TWAMP server.

Range: 1-65535

server-inactivity-timeout—Maximum time the TWAMP server has to finish the TWAMP control protocol negotiation. Control packet idle timeout value in minutes, 0 to disable (minutes).

Default: 15

Range: 0-30

Required Privilege Level

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

RELATED DOCUMENTATION

Two-Way Active Measurement Protocol (TWAMP) Overview | 917

Example: Configuring TWAMP Client and Server | 919

twamp-client

Syntax

```
twamp {
   client {
      control-connection name {
      authentication-mode none;
         destination-port;
         history-size;
         moving-average-size;
         target-address;
         test-count ;
         test-interval seconds;
         test-session name {
            target-address;
            data-fill-with-zeros;
            data-size;
            dscp-code-points;
            probe-count;
            probe-interval;
            thresholds;
            traps;
         }
         traps {
            control-connection-closed ;
            test-iteration-done ;
         }
         }
   }
}
```

Hierarchy Level

```
[edit services rpm twamp client]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Defines the Two-Way Active Measurement Protocol (TWAMP) client configuration. A client opens a TCP connection to the server on well-known port 862. The host that initiates the TCP connection takes the roles of control client and session sender. The host that acknowledges the TCP connection accepts the roles of server and session reflector.

Options

client—TWAMP client configuration.

authentication-mode—Set of authentication modes that the client can accept.

Default: none

destination-port—Either the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP) port to which a probe is sent.

Default: 862

history-size—Number of stored history entries.

Default: 50

Range: 0-500

moving-average-size—Number of samples for making statistical calculations.

Default: 0

Range: 0-1024

routing-instance—Routing instance used by test sessions.

target-address—Destination address or URL used for the probes.

test-count—Total number of test session iterations.

Default: 0

Range: 0-4,294,967,290

test-interval—Number of seconds to wait between tests.

Default: 1

Range: 1-255

test-session—Test session details.

data-fill-with-zeros—If the option is defined, then the test packet value becomes zero. If the option is not defined, then a pseudorandom number is updated as data.

dscp-code-points—DiffServ code point bits or alias used for UDP data of test probes or test packets in test sessions.

Default: 0

probe-count—Total number of probes per test.

Default: 1

Range: 1-4,294,967,290

thresholds—Test threshold values.

traps—Trap to send if threshold is met or exceeded.

control-connection-closed—Generate traps when the control connection is closed.

test-iteration-done—Generate traps when all test sessions under control connections complete one test iteration.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Two-Way Active Measurement Protocol (TWAMP) Overview | **917**

Example: Configuring TWAMP Client and Server | **919**

CHAPTER 76

Configuration Statements: Tracing and System Logging

IN THIS CHAPTER

- allow-duplicates | 2437
- archive (All System Log Files) | 2438
- archive (Individual System Log File) | 2440
- cache (Security Log) | 2442
- category (Security Logging) | 2443
- console (System Logging) | 2445
- critical-event (Process) | 2447
- critical-event (System) | 2448
- destination-override | 2449
- event-rate | 2450
- exclude (Security Log) | 2451
- exclude-hostname | 2452
- explicit-priority | 2453
- facility-override (Security) | 2454
- file (Security Log) | 2455
- file (System Logging) | 2457
- files | 2459
- filter (Security) | 2460
- format (Security Log) | 2461
- format (Security Log Stream) | 2462
- host (Security Log) | 2463
- host (System) | 2464
- idle-timeout (System) | 2467
- limit (Security Log) | 2468
- log (Security) | 2469
- log | 2474
- log-prefix (System) | 2476
- log-rotate-frequency | 2477

- major-event (System) | **2478**
- major-event (Process) | **2480**
- match | **2481**
- match-strings | **2483**
- memory (System) | **2484**
- minor-event (Process) | **2486**
- minor-event (System) | **2487**
- mode (Security Log) | **2489**
- no-remote-trace (System) | **2490**
- pic-services-logging | **2491**
- port (Syslog) | **2492**
- process (Memory) | **2493**
- rate-cap | **2495**
- rate-limit (Security Log) | **2496**
- report (Security Log) | **2498**
- security-log | **2501**
- security-log-percent-full | **2502**
- severity (Security Log) | **2503**
- size (System) | **2504**
- stream (Security Log) | **2505**
- structured-data | **2509**
- syslog (System) | **2510**
- system (Memory) | **2513**
- time-format | **2515**
- trace | **2517**
- traceoptions (Security Log) | **2519**
- traceoptions (System) | **2521**
- tracing | **2523**
- transport (Security Log) | **2524**
- ukern-trace | **2525**
- user (System Logging) | **2526**
- world-readable | **2527**

allow-duplicates

Syntax

allow-duplicates;

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog],
[edit logical-systems *logical-system-name* system syslog file *file-name*],
[edit logical-systems *logical-system-name* system syslog host *host-name*],
[edit logical-systems *logical-system-name* system syslog user *user-name*],
[edit system syslog],
[edit system syslog file *file-name*],
[edit system syslog host *host-name*],
[edit system syslog user *user-name*],

Release Information

Statement introduced in Junos OS Release 11.1.
Logical systems support introduced in Junos OS Release 11.4.

Description

Specify whether to allow the repeated messages in the system log output files. This can be set either at global configuration level or for individual file, host, or user. By default, this parameter is set to disable.

Options

file—Name of the file to log messages

host —Host to receive the messages

user—User to receive the notification of the event

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

archive (All System Log Files)

Syntax

```
archive <files number> <size size> <start-timetime> <transfer-interval interval>
   <binary-data | no-binary-data> <world-readable | no-world-readable>;
```

Hierarchy Level

```
[edit system syslog]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure archiving properties for all system log files.

Options

files *number*—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Range: 1 through 1000

Default: 10 files

size *size*—Maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***.

Syntax: ***x* k** to specify the number of kilobytes, ***x* m** for the number of megabytes, or ***x* g** for the number of gigabytes

Range: 64 KB through 1 GB

Default:

- 128 KB for EX Series switches

- 1 MB for M Series, MX Series, and T Series routers, OCX Series, and the QFX3500 switch, and SRX and vSRX series devices.
- 10 MB for TX Matrix and TX Matrix Plus routers

binary-data | no-binary-data—Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems)..

Default: no-binary-data

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

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

RELATED DOCUMENTATION

Specifying Log File Size, Number, and Archiving Properties | **1490**

archive (Individual System Log File)

Syntax

```
archive <archive-sites (ftp-url <password password>)> <files number> <size size> <start-time "YYYY-MM-DD.hh:mm">
    <transfer-interval minutes> <world-readable | no-world-readable>;
```

Hierarchy Level

```
[edit system syslog file filename]
```

Release Information

Statement introduced before Junos OS Release 7.4.
start-time and **transfer-interval** statements introduced in Junos OS Release 8.5.
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 archiving properties for a specific system log file.

Options

archive-sites *site-name*—FTP URL representing the destination for the archived log file (for information about how to specify valid FTP URLs, see *Format for Specifying Filenames and URLs in Junos OS CLI Commands*). If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the filename specified at the **[edit system syslog]** hierarchy level.

files *number*—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Range: 1 through 1000

Default: 10 files

password *password*—Password for authenticating with the site specified by the **archive-sites** statement.

size *size*—Maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***.

Syntax: ***x*k** to specify the number of kilobytes, ***x*m** for the number of megabytes, or ***x*g** for the number of gigabytes

Range: 64 KB through 1 GB

Default: 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers

start-time "*YYYY-MM-DD.hh*:*mm*"—Date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval *interval*—Interval at which to transfer the log file to an archive site.

Range: **5** through **2880** minutes

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: **no-world-readable**

Required Privilege Level

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

RELATED DOCUMENTATION

Specifying Log File Size, Number, and Archiving Properties | **1490**

cache (Security Log)

Syntax

```
cache {
    exclude exlude-name {
        destination-address destination-address;
        destination-port destination-port;
        event-id event-id;
        failure;
        interface-name interface-name;
        policy-name policy-name;
        process process-name;
        protocol protocol;
        source-address source-address;
        source-port source-address;
        success;
        user-name user-name;
    }
    limit value;
}
```

Hierarchy Level

```
[edit security log]
```

Release Information

Statement modified in Junos OS Release 9.2.

Description

Cache security log events in the audit log buffer.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

category (Security Logging)

Syntax

```
category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp | rtlog | pst-ds-lite | appqos
    | secintel)
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40. The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy levels introduced in Junos OS Release 18.3R1.

Description

Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.

Options

- **all**—All events are logged. By default, all the events listed in the **category** parameter are logged.
- **content-security**—Only content security events are logged.
- **fw-auth**—Firewall authentication events are logged.
- **screen**—Screen events are logged.
- **alg**—Application Layer Gateway (ALG) events are logged.
- **nat**—Network Address Translation (NAT) events are logged.
- **flow**—Flow events are logged.
- **sctp**—Stream Control Transmission Protocol (SCTP) events are logged.
- **gtp**—GPRS Tunneling Protocol (GTP) events are logged.
- **ipsec**—IPsec events are logged.
- **idp**—Intrusion Detection and Prevention (IDP) events are logged.
- **rtlog**—RTLOG system log events are logged.
- **pst-ds-lite**—PST dual-stack lite (DS-Lite) events are logged.

- **appqos**—Application quality of service (AppQoS) events are logged.
- **secintel**—Juniper Networks Security Intelligence (SecIntel) events are logged.

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

RELATED DOCUMENTATION

Application Security User Guide for Security Devices

Logical Systems and Tenant Systems User Guide for Security Devices

console (System Logging)

Syntax

```
console {
    facility severity;
}
```

Hierarchy Level

```
[edit system syslog]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the logging of system messages to the system console. Log messages include priority information, which is information about log messages' facility and severity levels.

Options

facility—Class (type) of messages to log. To specify multiple classes, include multiple ***facility severity*** statements.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. You can specify the minimum severity level of a message.

> **NOTE:** For a list of the facilities and message severities, see Table 147 on page 1470.

Required Privilege Level

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

RELATED DOCUMENTATION

Directing System Log Messages to the Console | 1531

System Log Explorer

critical-event (Process)

Syntax

```
critical-event {
    threshold process name memory-limit value ;
    action [snmp-trap | live-core | (terminate-process| terminate-process-force)];
}
```

Hierarchy Level

```
[edit system monitor memory process]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Indicates an event that, if left unchecked, may result in serious loss of service or interruption of traffic. You can specify the process threshold value for specific processes and their memory limit. When the threshold is crossed, you can configure the action to be performed. For instance, you can specify the process threshold for the **rpd** process and the memory limit for that process which you would classify as a critical event.

Options

threshold—Specifies the process threshold level for a minor event. You must specify the process name and the memory limit for the process.

memory— Specifies the permissible memory limit for the process after which the critical event is triggered.

action— Specifies the action to be performed when the threshold is crossed. For critical events, you can force terminate the process. You can also display a list of system core files created when the system failed which you can use to debug the issue. You can also raise an SNMP trap.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

System Log Explorer

critical-event (System)

Syntax

```
critical-event {
   threshold swap-usage value ;
   action [snmp-trap | live-vmcore | (RE-restart| RE-switchover)];
}
```

Hierarchy Level

```
[edit system monitor memory system]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Indicates an event that, if left unchecked, may result in serious loss of service or interruption of traffic. At the system level you can monitor the overall free pages (cache and free pages), kernel memory allocations and compare them with threshold values. You can also monitor the swap usage and specify the threshold for swap space usage. Most devices have a swap partition that you can configure to provide additional transient memory. Ideally, the swap partition is used only under exceptional circumstances. In current dynamic systems, you can sporadically use the swap partition as long as the usage is not high or persistent. For instance, you could categorise a critical event as one where the swap usage is greater than 75%.

You can only configure swap usage threshold for memory monitoring. If you do not configure the swap usage threshold, memory monitoring for swap usage is based on the default threshold. Memory monitoring for other features is based on the default threshold.

Options

threshold—Specifies the process threshold level for a minor event. You must specify the process name and the memory limit for the process.

swap-usage—Specifies the swap usage in percentage.

action—Specifies the action to be performed when the threshold is crossed.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

System Log Explorer

destination-override

Syntax

```
destination-override {
    syslog host ip-address;
}
```

Hierarchy Level

```
[edit system tracing]
```

Release Information

Statement introduced in Junos OS Release 9.2.

Description

This option overrides the system-wide configuration under **[edit system tracing]** and has no effect if system tracing is not configured.

Options

These options specify the system logs and the host to which remote tracing output is sent:

- **syslog**—Specify the system process log files to send to the remote tracing host.
- **host *ip-address***—Specify the IP address to which to send tracing information.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Tracing and Logging Operations

tracing | 2523

event-rate

Syntax

```
event-rate rate;
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement introduced in Junos OS Release 10.0.
The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Limits the rate at which logs will be streamed per second.

Options

rate—Rate at which logs will be streamed per second.

Range: 0 through 1500 logs per second

Default: 1500 logs per second

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | **2510**

exclude (Security Log)

Syntax

```
exclude exlude-name {
    destination-address destination-address;
    destination-port destination-port;
    event-id event-id;
    failure;
    interface-name interface-name;
    policy-name policy-name;
    process process-name;
    protocol protocol;
    source-address source-address;
    source-port source-port;
    success;
    user-name user-name;
}
```

Hierarchy Level

```
[edit security log cache]
[edit logical-systems name security log cache]
[edit tenants tenant-name security log cache]
```

Release Information

Statement introduced in Junos OS Release 11.2.
The [edit **logical-systems** *name* security log cache] and [edit **tenants** *tenant-name* security log cache] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Configure a list of auditable events that can be excluded from the audit log.

Options

- **destination-ip *destination-address***—Destination IP address.
- **destination-port *destination-port***—Destination port number.
- **event-id *event-id***—Error message identification number.
- **failure**—Failed audit event logs.
- **interface-name *interface-name***—Name of the interface.
- **policy-name *policy-name***—Policy name filter.
- **process *process-name***—Process that generated the event.

- **protocol *protocol***—Protocol that generated the event.
- **source-ip *source-address***—Source IP address.
- **source-port *source-port***—Source port number.
- **success**—Successful audit event logs.
- **username *user-name***—User name filter.

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

RELATED DOCUMENTATION

show security log | 2944
clear security log | 2922

exclude-hostname

Syntax

```
exclude-hostname;
```

Hierarchy Level

```
[edit system syslog host hostname]
```

Release Information
Statement introduced in Junos OS Release 13.2

Description
Disable logging of hostname in the message directed to remote host.

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

explicit-priority

Syntax

```
explicit-priority;
```

Hierarchy Level

```
[edit logical-systems logical-system-name system syslog file filename],
[edit logical-systems logical-system-name system syslog host],
[edit system syslog file filename],
[edit system syslog host]
```

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

Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination.

When the **structured-data** statement is also included at the **[edit system syslog file *filename*]** hierarchy level, this statement is ignored for the file.

Required Privilege Level

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

RELATED DOCUMENTATION

- Including Priority Information in System Log Messages | **1492**
- System Log Explorer
- structured-data | **2509**

facility-override (Security)

Syntax

```
facility-override facility;
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D35 for SRX Series devices.

The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Alternate facility for logging to remote host.

System log server is set up to use a facility-override value to filter or write log files received by a system log agent.

Required Privilege Level

system—To view this statement in the configuration.

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

file (Security Log)

Syntax

```
file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
}
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement modified in Junos OS Release 9.2.
The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Configure security log file options for logs in binary format.

Options

- **files *number***—Specify the maximum number of binary log files.

Range: 2 through 10 files.

- **name *name*** —Name of the file to log messages.
- **path *filepath***—Specify the path of the binary log file.
- **size *maximum-file-size***—Maximum size of each trace file, in megabytes (MB).

Range: 1 KB through 10 MB

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

file (System Logging)

Syntax

```
file filename {
    facility severity;
    archive {
        files number;
        size size;
        (no-world-readable | world-readable);
    }
    explicit-priority;
    match "regular-expression";
    match-strings string-name;
    structured-data {
        brief;
    }
}
```

Hierarchy Level

```
[edit system syslog]
```

Release Information

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

Description

Configure the logging of system messages to a file.

Options

facility—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Table 147 on page 1470.

file *filename*—File in the **/var/log** directory in which to log messages from the specified facility. To log messages to more than one file, include more than one **file** statement.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 148 on page 1471.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Directing System Log Messages to a Log File | 1530

files

Syntax

```
files number;
```

Hierarchy Level

```
[edit system syslog archive],
[edit system syslog file filename archive]
```

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 EX Series switches.

Description

Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it to ***logfile*.0.gz** (for information about the maximum file size, see **size**). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Options

number—Maximum number of archived files.

Range: 1 through 1000

Default: 10 files

Required Privilege Level

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

RELATED DOCUMENTATION

size | 2504

filter (Security)

Syntax

```
filter threat-attack
```

Hierarchy Level

```
[edit security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

Description

Configure the log stream filter to transmit only threat and attack logs to the ClearPass Policy Manager (CPPM). The integrated ClearPass authentication and enforcement feature sends to the CPPM threat and attack logs detected by the SRX Series device security modules. You can use these reports to inform your approach to hardening the CPPM security policy. Setting the log stream filter to threat-attack ensures that the SRX Series device and the log server are not overburdened by irrelevant logs.

NOTE: Unlike for other features that use a filter for log streams, threat-attack is the only log stream filter supported for integrated ClearPass. Therefore, it is not shown here as an option.

Required Privilege Level

security—To view this statement in the configuration.

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

format (Security Log)

Syntax

```
format (binary | sd-syslog | syslog)
```

Hierarchy Level

```
[edit security log]
```

Release Information

Statement introduced prior to Junos OS Release 10.0. Statement updated in Junos OS Release 12.1.

Description

Set the default log format for event mode security logging on the device.

Options

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.

Default: syslog.

Required Privilege Level

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

RELATED DOCUMENTATION

log (Security) | 2469

format (Security Log Stream)

Syntax

```
format (binary | sd-syslog | syslog | welf)
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 10.0 . Updated in Junos OS Release 12.1 .
The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.3R1.

Description

Set the format for remote security message logging to **binary**, **syslog** (system log), **sd-syslog** (structured system log), or **welf**. Note that for the WELF format, the category must be set to **content-security** (see **category (Security Logging)**).

Options

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.
- **welf**—Web Trends Extended Log Format.

Default: By default **syslog** (system log) is enabled.

Required Privilege Level

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

RELATED DOCUMENTATION

Application Security User Guide for Security Devices

Logical Systems and Tenant Systems User Guide for Security Devices

host (Security Log)

Syntax

```
host {
    ip-address;
    port port-number;
}
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 9.2.

Description

You can specify the IP address of the server to which the security logs are streamed.

The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.

The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy levels introduced in Junos OS Release 18.3R1.

Options

- *ip-address*—Specify IP address of the host.
- **port** *port-number*—Specify host port number.

Default: The default destination port is the system log port. For UDP or TCP, the default port is 514. For TLS, the default port is 6514.

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

host (System)

Syntax

```
host (hostname | other-routing-engine) {
    facility severity;
    exclude-hostname
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    match-strings string-name;
    source-address source-address
    structured-data {
        brief;
    }
}
```

QFX Series and OCX Series

```
host (hostname {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    match-strings string-name;
    port;
    source-address source-address
}
```

TX Matrix Router and EX Series Switches

```
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
```

```
    match-strings string-name;
    port;
    source-address source-address
}
```

TX Matrix Plus Router

```
host (hostname | other-routing-engine | sfc0-master) {
    facility severity;
    allow-duplicates;
    explicit-priority;
    facility-override facility;
    log-prefix (System) string;
    match "regular-expression";
    match-strings string-name;
    port;
    source-address source-address
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name system syslog],
[edit system syslog]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the logging of system messages to a remote destination.

Options

facility—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Table 147 on page 1470.

hostname—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a **host** statement for each one.

other-routing-engine—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.

> **NOTE:** The **other-routing-engine** option is not applicable to the QFX Series and OCX Series.

port—Port number of the remote syslog server that can be modified.

scc-master—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 148 on page 1471.

sfc0-master—(TX Matrix Plus routers only) On a T1600 or T4000 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Directing System Log Messages to a Remote Machine or the Other Routing Engine | **1532**
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router | **1541**
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router | **1542**

idle-timeout (System)

Syntax

```
idle-timeout idle-timeout;
```

Hierarchy Level

```
[edit system login]
```

Release Information

Statement introduced in Junos OS Release 16.1 for the M Series, MX Series, and PTX Series.
Statement introduced in Junos OS Release 15.1X49-D70 for the vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.
Statement introduced in Junos OS Release 17.4R1-S1 for the SRX4600 devices.

Description

Configure the maximum time for which the C shell or CLI console session can be idle. The user (including the root user) is logged out after the expiry of **idle-timeout**.

Options

idle-timeout— Maximum idle time before logout.

Range: 1 through 60 minutes

Required Privilege Level

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

limit (Security Log)

Syntax

```
limit value;
```

Hierarchy Level

```
[edit security log cache]
[edit logical-systems name security log cache]
[edit tenants tenant-name security log cache]
```

Release Information

Statement modified in Junos OS Release 9.2.
The [edit **logical-systems** *name* security log cache] and [edit **tenants** *tenant-name* security log cache] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Specify the number of security log entries to be kept in memory.

Options

Once the maximum value limit is reached, new entries will not be added until the cache size drops.

Range: 0 through 4,294,967,295

Default: 10,000 security log entries.

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | **2510**

log (Security)

Syntax

```
log {
    (source-address source-address | source-interface source-interface);
    cache {
        exclude name {
            destination-address destination-address;
            destination-port destination-port;
            event-id event-id;
            failure;
            interface-name interface-name;
            policy-name policy-name;
            process process;
            protocol protocol;
            source-address source-address;
            source-port source-port;
            success;
            username username;
        }
        limit limit;
    }
    disable;
    escape;
    time-format (year | millisecond);
    event-rate logs per second;
    facility-override (authorization | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 |
        local7 | user);
    file {
        files files;
        name name;
        path path;
        size size;
    }
    format (binary | sd-syslog | syslog);
    max-database-record max-database-record;
    message-rate-limit messages per second;
    mode (event | stream | stream-event);
    rate-cap logs per second;
    report {
        logs-per-table {
            idp idp;
            ipsec-vpn ipsec-vpn;
            screen screen;
```

```
        session-all session-all;
        sky sky;
        utm utm;
    }
    table-lifetime table-lifetime;
    table-mode {
        dense;
    }
}
root-streaming;
stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp | rtlog |pst-ds-lite |
        appqos |secintel |aamw);
    filter {
        threat-attack;
        }
    format (binary | sd-syslog | syslog | welf);
    host {
        ip-address;
        port port-number;
        routing-instanceinstance-name;
    }
    rate-limit {
        log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
    source-address {
        ip-address;
    }
    time-format (year | millisecond);
    transport {
        protocol (tcp | tls | udp);
        tcp-connections tcp-connections;
        tls-profile tls-profile;
    }
}
traceoptions {
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
    flag name;
    no-remote-trace;
}
```

```
    transport {
        protocol (tcp | tls | udp);
        tcp-connections tcp-connections;
        tls-profile tls-profile;
    }
    utc-timestamp;
}
```

Hierarchy Level

```
[edit security]
[edit logical-systems name security]
[edit tenants tenant-name security]
```

Release Information

Statement introduced in Junos OS Release 9.2.
The [edit **logical-systems** *name* security] and [edit **tenants** *tenant-name* security] hierarchy levels introduced in Junos OS Release 19.1R1.
escape option added in Junos OS Release 20.2R1.
root-streaming option added in Junos OS Release 20.3R1.

Description

Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options

cache—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

escape—Escapes the stream log forwarding to avoid parsing errors. Stream mode supports escape in **sd-syslog** and **binary** format. Event mode supports escape only in **binary** format.

time-format—Specify the year, the millisecond, or both in the timestamp.

event-rate *rate*—Limit the rate at which logs are streamed per second.

Range: 0 through 1500

Default: 1500

facility-override—Alternate facility for logging to remote host.

file—Specify the security log file options for logs in binary format.

Values:

- ***max-file-number***—Maximum number of binary log files.
  - The range is 2 through 10 and the default value is 10.
- ***file-name***—Name of binary log file.
- ***binary-log-file-path***—Path to binary log files.
- ***maximum-file-size***—Maximum size of binary log file in megabytes.
  - The range is 1 through 10 and the default value is 10.

format—Set the security log format for the device.

max-database-record—The following are the disk usage range limits for the database:

Range:

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

Default:

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000

Be sure there is enough free space in **/var/log/hostlogs/**, otherwise logs might be dropped when written into the database.

mode—Control how security logs are processed and exported.

rate-cap *rate-cap-value*—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

Range: 0 through 5000 logs per second

Default: 5000 logs per second

root-streaming—Allows the user logical systems to generate the logs using the root logical system's stream configuration.

source-address ***source-address***—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface ***interface-name***—Specify a source interface name, which is mandatory to configure *stream host*.

The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

log

Syntax

```
log {
    all;
    errors;
    info;
    sessions-allowed;
    sessions-dropped;
    sessions-ignored;
    sessions-whitelisted;
    warning;
}
```

Hierarchy Level

[edit services ssl proxy profile *profile-name* actions]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10.

Description
Specify the logging actions. When configuring SSL proxy, you can choose to set the option to receive some or all of the logs.

SSL proxy logs contain the logical system name, SSL proxy allowlists, policy information, SSL proxy information, and other information that helps you troubleshoot when there is an error.

You can configure logging of all or specific events, such as error, warning, and information events. You can also configure logging of sessions that are allowlisted, dropped, ignored, or allowed after an error occurs.

Options

- **all**—Log all events.
- **errors**—Log all error events.
- **info**—Log all information events.
- **sessions-allowed**—Log SSL session allowed events after an error.
- **sessions-dropped**—Log only SSL session dropped events.
- **sessions-ignored**—Log session ignored events.
- **sessions-whitelisted**—Log SSL session allowlisted events.

- **warning**—Log all warning events.

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

RELATED DOCUMENTATION

Configuring SSL Forward Proxy

log-prefix (System)

Syntax

```
log-prefix string;
```

Hierarchy Level

```
[edit system syslog host]
```

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

Include a text string in each message directed to a remote destination.

Options

string—Text string to include in each message.

Required Privilege Level

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

RELATED DOCUMENTATION

Adding a Text String to System Log Messages Directed to a Remote Destination | 1535

log-rotate-frequency

Syntax

```
log-rotate-frequency frequency;
```

Hierarchy Level

```
[set system syslog]
```

Release Information

Statement introduced in Junos OS Release 11.3.

Description

Configure the system log file rotation frequency by configuring the time interval for checking the log file size.

When the log file size has exceeded the configured limit, the old log file is archived and a new log file is created.

Options

frequency—Frequency of rotation of the system log file.

Range: 1 minute through 59 minutes

Default: 15 minutes

Required Privilege Level

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

RELATED DOCUMENTATION

Specifying Log File Size, Number, and Archiving Properties | **1490**

syslog | **2510**

major-event (System)

Syntax

```
major-event {
   threshold swap-usage value ;
   action [snmp-trap | live-vmcore];
}
```

Hierarchy Level

```
[edit system monitor memory system]
```

Release Information
Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description
Indicates an event that, if left unchecked, may result in significant loss of service or interruption of traffic. At the system level you can monitor the overall free pages (cache and free pages), kernel memory allocations and compare them with threshold values. You can also monitor the swap usage and specify the threshold for swap space usage. Most devices have a swap partition that you can configure to provide additional transient memory. Ideally, the swap partition is used only under exceptional circumstances. In current dynamic systems, you can sporadically use the swap partition as long as the usage is not high or persistent. For instance, you could categorise a major event as one where the swap usage is greater than 50%. If the threshold value is crossed, then you can raise an SNMP trap or display a list of system core files created when the system failed which can be used to debug the issue.

You can only configure swap usage threshold for memory monitoring. If you do not configure the swap usage threshold, memory monitoring for swap usage is based on the default threshold. Memory monitoring for other features is based on the default threshold.

Options

threshold—Specifies the process threshold level for a major event. You must specify the process name and the memory limit for the process.

swap-usage—Specifies the swap usage in percentage.

action—Specifies the action to be performed when the threshold is crossed. You can either

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

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

System Log Explorer

major-event (Process)

Syntax

```
major-event {
   threshold process name memory-limit value ;
   action [snmp-trap | live-core | (terminate-process| terminate-process-force)];
}
```

Hierarchy Level

```
[edit system monitor memory process]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Indicates an event that, if left unchecked, may result in significant loss of service or interruption of traffic. You can specify the process threshold value for specific processes and their memory limit. When the threshold is crossed, you can configure the action to be performed. For instance, you can specify the threshold for the **rpd** process and the memory limit for that process which you would classify as a a major event.

Options

threshold— Specifies the process threshold level for a major event. You must specify the process name and the memory limit for the process.

memory— Specifies the permissible memory limit for the process after which the major event is triggered.

action— Specifies the action to be performed when the threshold is crossed. For major events, you can raise an SNMP trap or terminate the process. You can also display a list of system core files created when the system failed which you can use to debug the issue.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

System Log Explorer

match

Syntax

```
match "regular-expression";
```

Hierarchy Level

```
[edit logical-systems logical-system-name system syslog file filename],
[edit logical-systems logical-system-name system syslog user (username | *)],
[edit system syslog file filename],
[edit system syslog host hostname | other-routing-engine| scc-master)],
[edit system syslog user (username | *)]
```

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

Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.

If you configure both the **match** and **match-strings** statements for the same destination, Junos OS evaluates the **match-strings** condition first, and if the condition is satisfied, then the message is logged and the **match** condition is not evaluated. If the condition in the **match-strings** statement is not satisfied, then the system evaluates the regular expression in the **match** configuration statement.

Options

regular-expression—Regular expression against which to match messages to log.

> The regular expressions must use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions and must not contain a slash (/) or a percent sign (%).

Required Privilege Level

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

RELATED DOCUMENTATION

Using Strings and Regular Expressions to Refine the Set of Logged Messages | 1497

match-strings

Syntax

```
match-strings string;
```

```
match-strings [string1 string2];
```

Hierarchy Level

```
[edit system syslog file filename],
[edit system syslog host hostname],
[edit system syslog user username]
```

Release Information

Statement introduced in Junos OS Release 16.1.

Description

Specify a text substring that must appear in a message that is logged to a destination. If multiple strings are configured, the message is logged to the given destination if any of the substrings are matched.

The **match-strings** statement performs a simple string comparison, and as a result, it is less CPU-intensive than using the **match** statement to match against complex regular expressions. If you configure both the **match** and **match-strings** statements for the same destination, Junos OS evaluates the **match-strings** condition first; if the message includes any of the configured substrings, then the message is logged and the **match** condition is not evaluated. If the **match-strings** condition is not satisfied, then the system evaluates the message against the regular expression in the **match** configuration statement.

Options

string—String or list of strings against which to match messages to log.

Range: 1 through 50 strings

Range: 1 through 1020 characters per string

Required Privilege Level

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

RELATED DOCUMENTATION

Using Strings and Regular Expressions to Refine the Set of Logged Messages | 1497

memory (System)

Syntax

```
memory {
   system {
      frequency (minutes | hours| days) <value>;
      minor event {
         threshold swap usage <value in percentage>;
         action snmp-trap;
      }
      major event {
         threshold swap usage <value in percentage>;
         action [snmp-trap | live-vmcore];
      }
      critical event {
         threshold swap usage <value in percentage>;
         action [snmp-trap | live-vmcore| (RE-restart| RE-switchover) ];
      }
   }
   process (Memory) {
   frequency (minutes | hours| days) <value>;
      minor event {
         threshold <process-name> memory-limit <memory-limit-in MBs>;
         action snmp-trap;
      }
      major event {
         threshold <process-name> memory-limit <memory-limit-in MBs>;
         action [ snmp-trap |live-core | (terminate-process | terminate-process-force)] ;
      }
      critical event {
         threshold <process-name> memory-limit <memory-limit-in MBs>;
         action [ snmp-trap |live-core | (terminate-process | terminate-process-force)] ;
      }
}
```

Hierarchy Level

```
[edit system monitor]
```

Release Information

Statement introduced in Junos OS Release 20.1R1 for MX Series and PTX Series routers.

Description

Configure the memory monitoring system on your PTX and MX Series routers. The memory monitoring system on your device monitors anomalies with respect to the memory utilization of Junos applications and overall system in the control plane of your device. Apart from monitoring the system memory, you can also configure the device to monitor the per-process memory footprint as well to help detect possible leaks and take configured action.

Memory can be exhausted when there is over scaling, for instance when you test a high scale on a device that does support the scale because of physical resource limitations. Memory can also be exhausted when there are temporary spikes for example when a new FIB object is added before the older FIB objects are deleted. These temporary spikes are usually transient and resolve after a while. Also, a memory leak in any one of the applications or even in the kernel can lead to memory exhaustion. So, it is necessary that you monitor memory usage across applications and the kernel.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

minor-event (Process)

Syntax

```
minor-event {
    threshold process name memory-limit value ;
    action snmp-trap;
}
```

Hierarchy Level

```
[edit system monitor memory process]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Indicates a non-critical event that, if left unchecked, may cause an interruption in service or degradation in performance but does not significantly affect the device. You can specify the process threshold value for specific processes and their memory limit. When the threshold is crossed, you can configure the action to be performed. For instance, you can specify the process threshold for the **rpd** process and the memory limit for that process. If the system detects that the memory utilized by the process is greater than the threshold memory limit, based on the value, a minor event is triggered. Usually, for minor events, an SNMP trap is raised.

Options

threshold— Specifies the process threshold level for a minor event. You must specify the process name and the memory limit for the process.

memory— Specifies the permissible memory limit for the process after which the minor event is triggered.

action— Specifies the action to be performed when the threshold is crossed. Usually, in case of minor events, an SNMP trap is raised.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

System Log Explorer

minor-event (System)

Syntax

```
minor-event {
    threshold swap-usage value ;
    action snmp-trap ;
}
```

Hierarchy Level

```
[edit system monitor memory system]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Indicates a non-critical event that, if left unchecked, may cause an interruption in service or degradation in performance but does not significantly affect the device. You can monitor the swap usage and specify the threshold for swap space usage. Most devices have a swap partition that you can configure to provide additional transient memory. Ideally, the swap partition is used only under exceptional circumstances. In current dynamic systems, you can sporadically use the swap partition as long as the usage is not high or persistent. For instance, you could categorise a minor event as one where the swap usage is greater than 20%.

You can only configure swap usage threshold for memory monitoring. If you do not configure the swap usage threshold, memory monitoring for swap usage is based on the default threshold. Memory monitoring for other features is based on the default threshold.

Options

threshold— Specifies the process threshold level for a minor event. You must specify the process name and the memory limit for the process.

swap-usage— Specifies the swap usage in percentage.

action— Specifies the action to be performed when the threshold is crossed.

Required Privilege Level

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

RELATED DOCUMENTATION

System Log Explorer

mode (Security Log)

Syntax

```
mode (event | stream | stream-event)
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement introduced in Junos OS Release 10.0.
The [edit **logical-systems** *name* security log] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log] hierarchy level introduced in Junos OS Release 18.3R1.
stream-event option is introduced in Junos OS Release 20.2R1 for SRX Series devices.

Description

Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server).

Options

- **event**— Process security logs in the control plane.
- **stream**— Process security logs directly in the forwarding plane.
- **stream-event**— Process security logs in the control and forwarding plane.

Default:

- event is a default mode on SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, SRX650, and SRX1500 devices.

  Starting in Junos OS Release 19.3R1, the default mode for system log messages for SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M devices is changed from event mode to stream mode.

- stream is a default mode on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800, SRX4100, and SRX4200 devices.

> **NOTE:** Starting with Junos OS Release 15.1X49-D140, the default mode for SRX1500 device is stream mode. Prior to Junos OS Release 15.1X49-D140, the default mode for SRX1500 device was event mode.

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

RELATED DOCUMENTATION

syslog (System) | 2510

no-remote-trace (System)

Syntax

```
no-remote-trace;
```

Hierarchy Level

```
[edit system scripts commit traceoptions]
```

Release Information
Statement introduced in Junos OS Release 11.2.

Description
Disable remote tracing.

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

RELATED DOCUMENTATION

traceoptions (Security Datapath Debug) | 2009

pic-services-logging

Syntax

```
pic-services-logging {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Enable PICs to send special logging information to the Routing Engine for archiving on a hard disk.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the PIC services logging process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, the device reboots from the secondary Routing Engine.

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

port (Syslog)

Syntax

```
port port number;
```

Hierarchy Level

```
[edit system syslog host hostname | other-routing-engine| scc-master)]
```

Release Information

Statement introduced in Junos OS Release 11.3.

Description

Specify the port number for the remote syslog server.

Options

port number—Port number of the remote syslog server.

Range: 0 through 65535

Default: 514

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

syslog | 2510

host | 2464

process (Memory)

Syntax

```
process {
   frequency (minutes | hours | days) value;
   minor-event {
      threshold process name memory-limit value ;
      action snmp-trap;
   }
   major-event {
      threshold process name memory-limit value ;
      action [snmp-trap | live-core | (terminate-process| terminate-process-force)];
   }
   critical-event {
      threshold process name memory-limit value ;
      action [snmp-trap | live-core | (terminate-process| terminate-process-force)];
   }
}
```

Hierarchy Level

```
[edit system monitor memory]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Configure process level memory monitoring. Because you cannot specify a threshold for all processes, an algorithm (heuristics-based) is used to identify the processes that are likely to cross the threshold. The algorithm can identify the processes based on learning the memory growth pattern of the processes and comparing the memory usage of the processes with the baseline of the process. The algorithm measures the virtual memory footprint, increase in memory foot print since baseline, and memory growth pattern score to identify the processes. You can also specify exceptions. Learning is always on at the configured time interval for process monitoring. Also, prediction is possible only when the module is aware that the system is running low on memory.

The remaining statements are explained separately.

Options

frequency—Specify the frequency of system level memory monitoring. You can specify the frequency in days, hours or minutes. Possible values: 1 through 65535.

minor-event— Indicates a non-critical event that, if left unchecked, may cause an interruption in service or degradation in performance but does not significantly affect the device.

major-event— Indicates an event that, if left unchecked, may result in significant loss of service or interruption of traffic.

critical-event— Indicates an event that, if left unchecked, may result in serious loss of service or interruption of traffic. In case a critical event is triggered, you can terminate the process but only if the device is running out of memory.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

System Log Explorer

rate-cap

Syntax

```
rate-cap <rate-cap-value>;
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement introduced in Junos OS Release 10.0.

The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Limits the rate at which data plane logs will be generated per second.

Options

rate-cap *rate-cap-value*—Works with event mode only. Limits the rate at which data plane logs will be generated per second

Range: 0 through 5000 logs per second

Default: 5000 logs per second

Required Privilege Level

security—To view this statement in the configuration.

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

RELATED DOCUMENTATION

syslog (System) | **2510**

rate-limit (Security Log)

Syntax

```
rate-limit rate-limit;
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.
The [edit **logical-systems** *name* security log stream] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream] hierarchy level introduced in Junos OS Release 18.3R1.

Description

The Integrated Authentication and Enforcement feature sends threat and attack logs generated by the SRX Series device security modules to the ClearPass Policy Manager (CPPM) to use in its security policy assessment.

The logs are sent in stream mode. To avoid overburdening the SRX Series device and the log server, you can control the rate at which these logs are sent. By setting a rate-limit value, you can constrain the number of logs that are sent in 1 second. After the limit is reached, no more logs are sent.

Range: 1 through 65,535.

NOTE: For devices with multicore systems that use SPUs, each SPU is programmed with the configured-rate, which results in an aggregate-rate proportional to the number of SPUs.

```
SPU configured-rate = aggregate-rate/number-of-SPUs
```

Rate limiting on SRX5400, SRX5600, and SRX5800 devices is generally not as accurate as it is on SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, and SRX4200 devices, because the generation of logs is not entirely balanced between SPUs.

Required Privilege Level

security—To view this statement in the configuration.

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

report (Security Log)

Syntax

```
report {
    logs-per-table {
        idp log-number;
        ipsec-vpn log-number;
        screen log-number;
        session-all log-number;
        sky log-number;
        utm log-number;
    }
    table-lifetime table-lifetime;
}
    table-mode {
        dense;
    }
```

Hierarchy Level

[edit security **log (Security)**]
[edit logical-systems *name* security **log (Security)**]
[edit tenants *tenant-name* security **log (Security)**]

Release Information

Statement introduced in Junos OS Release 15.1X49-D100
The [edit **logical-systems** *name* security **log (Security)**] and [edit **tenants** *tenant-name* security **log (Security)**] hierarchy levels introduced in Junos OS Release 19.1R1.
table-mode option added in Junos OS Release 19.4R1.

Description

Set security log report settings.

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action.

The on-box reporting feature is enabled by default on a SRX Series device with Junos OS Release 15.1X49-D100 or later.

If you are upgrading your SRX Series device from a Junos OS Release prior to Junos OS 15.1X49-D100, then on-box reporting feature is disabled by default. You need to run the **set security log report** command to enable the on-box reporting feature on the device.

Options

report—Enable log report.

logs-per-table—Log number for each table.

idp—Log number of idp.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 40000 through 80000

Default: 40000

Range: For SRX1500, SRX4100, and SRX4200: 500000 through 1000000

Default: 500000

Range: For SRX4600: 1333333 through 2666666

Default: 1333333

ipsec-vpn—Log number of IPsec-VPN.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 26666 through 26666

Default: 26666

Range: For SRX1500, SRX4100, and SRX4200: 333333 through 333333

Default: 333333

Range: For SRX4600: 666666 through 666666

Default: 666666

screen—Log number of screen.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 40000 through 80000

Default: 40000

Range: For SRX1500, SRX4100, and SRX4200: 500000 through 1000000

Default: 500000

Range: For SRX4600: 1333333 through 2666666

Default: 1333333

session-all—Log number of session.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 80000 through 800000

Default: 80000

Range: For SRX1500: 533333 through 5333333

Default: 533333

Range: For SRX4100 and SRX4200: 666666 through 6666666

Default: 666666

Range: For SRX4600: 1000000 through 10000000

Default: 1000000

sky—Log number of SKY.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 40000 through 80000

Default: 40000

Range: For SRX1500, SRX4100, and SRX4200: 500000 through 1000000

Default: 500000

Range: For SRX4600: 1333333 through 2666666

Default: 1333333

utm—Log number of UTM.

Range: For SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and vSRX: 40000 through 80000

Default: 40000

Range: For SRX1500, SRX4100, and SRX4200: 500000 through 1000000

Default: 500000

Range: For SRX4600: 1333333 through 2666666

Default: 1333333

table-lifetime—Table lifetime days.

Default: 90

Range: 0 through 365

table-mode—Enable table dense mode.

Required Privilege Level

The remaining statements are explained separately. See CLI Explorer.

RELATED DOCUMENTATION

log (Security) | **2469**

security-log

Syntax

```
security-log {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the security log process.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the security log process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | 2510

security-log-percent-full

Syntax

```
security-log-percent-full percentage;
```

Hierarchy Level

```
[edit security alarms potential-violation]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Raise a security alarm when security log exceeds a specified percent of total capacity.

Options

percentage—Percentage of security log capacity at which a security alarm is raised.

Range: 0 through 100 percent

Required Privilege Level

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

RELATED DOCUMENTATION

syslog (System) | **2510**

severity (Security Log)

Syntax

```
severity (alert | critical | debug | emergency | error | info | notice | warning)
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement modified in Junos OS Release 9.2.

The [edit **logical-systems** *name* security log stream *stream-name*] and [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Set severity threshold for security logs.

Options

- **alert**— Conditions that require immediate attention.
- **critical**—Critical conditions.
- **debug**—Information normally used in debugging.
- **emergency**—Conditions that cause security functions to stop.
- **error**—General error conditions.
- **info**—Information about normal security operations.
- **notice**—Nonerror conditions that are of interest.
- **warning**—General warning conditions.

Default: debug.

Required Privilege Level

security—To view this statement in the configuration.

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

RELATED DOCUMENTATION

syslog (System) | 2510

size (System)

Syntax

```
size size;
```

Hierarchy Level

```
[edit system syslog archive],
[edit system syslog file filename archive]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***. For information about the number of archive files that the utility creates in this way, see **files**.

Options

size—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Syntax: ***x*k** to specify the number of kilobytes, ***x*m** for the number of megabytes, or ***x*g** for the number of gigabytes

Range: 64 KB through 1 GB

Default: 1 MB for MX Series routers the QFX Series, and the OCX Series

Required Privilege Level

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

RELATED DOCUMENTATION

Specifying Log File Size, Number, and Archiving Properties | **1490**
System Log Explorer
files | **2459**

stream (Security Log)

Syntax

```
stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp | rtlog |pst-ds-lite | appqos
        |secintel |aamw);
    filter {
        threat-attack;
        }
    format (binary | sd-syslog | syslog | welf);
    host {
        ip-address;
        port port-number;
        routing-instanceinstance-name;
    }
    rate-limit {
        log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
    source-address {
        ip-address;
    }
    time-format (year | millisecond);
    transport {
        protocol (tcp | tls | udp);
        tcp-connections tcp-connections;
        tls-profile tls-profile;
    }
}
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement modified in Junos OS Release 9.2.

The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

time-format, **source-address**, and **transport** options are introduced in Junos OS Release 20.2R1.

Description

Defines the TWAMP server configuration settings.

Options

stream—Every stream can configure file or host.

Values:

- **category**— Type of events that may be logged.
  - **all**— All events are logged
  - **content-security** — Content security events are logged
  - **fw-auth**— Fw-auth events are logged.
  - **screen**— Screen events are logged.
  - **alg**— Alg events are logged.
  - **nat**— Nat events are logged.
  - **flow**— Flow events are logged.
  - **sctp**— Sctp events are logged.
  - **gtp**— Gtp events are logged.
  - **ipsec**— IPsec events are logged.
  - **idp**— Idp events are logged.
  - **rtlog**— Rtlog events are logged.
  - **pst-ds-lite**— Pst-ds-lite events are logged.
  - **appqos**— Appqos events are logged.
  - **secintel**— AAMW events are logged.
- **filter *threat-attack***— Selects the filter to filter the threat attack security events to be logged
- **format *(binary | sd-syslog | syslog)***— Specify the log stream format in binary or sd-syslog or syslog formats.
- **host *ip-address***— Destination to send security logs.
  - **port**— Specify the host port number.
  - **routing-instance**— Specify the routing instance name.
- **rate-limit *rate***— Specify the rate limit for security logs.
  - The range is 1 through 65535 logs per second and the default value is 65535
- **severity**— Specify the severity threshold for security logs.
  - **alert**— Specify the conditions that require immediate attention.
  - **critical**— Specify the critical conditions.
  - **debug**— Specify the information normally used in debugging.

  - **emergency**— Specify the conditions that cause security functions to stop.
  - **error**— Specify the general error conditions.
  - **info**— Specify the Information about normal security operations.
  - **notice**— Specify the non error conditions that are of interest.
  - **warning**— Specify the general warning conditions.
- **source-address**— Specify the source address to the stream log.
- **time-format *(year | millisecond)***— Specify the year, the millisecond, or both in the timestamp.
- **transport**— Set the security log transport settings.
  - **protocol *(tcp | tls | udp)***— Specify the security log transport protocol for the device. Values: tcp, tls, and udp.
  - **tcp-connections**— Specify the number of tcp connections per stream. Values: 1 through 5.

    NOTE: **tcp-connections** is not supported on logical and tenant systems.

  - **tls-profile**— Specify the tls profile.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Example: Configuring AppTrack

category (Security Logging) | **2443**

structured-data

Syntax

```
structured-data {
    brief;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog file *filename*],
[edit system syslog file *filename*]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol* (http://tools.ietf.org/html/draft-ietf-syslog-protocol-23).

> **NOTE:** When this statement is included, other statements that specify the format for messages written to the file are ignored (the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level and the **time-format** statement at the **[edit system syslog]** hierarchy level).

Required Privilege Level

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

RELATED DOCUMENTATION

Logging Messages in Structured-Data Format | 1489
explicit-priority | 2453
time-format | 2515

syslog (System)

Syntax

```
syslog {
    allow-duplicates;
    archive {
        (binary-data| no-binary-data);
        files number;
        size maximum-file-size;
        start-time "YYYY-MM-DD.hh:mm";
        transfer-interval minutes;
        (world-readable | no-world-readable);
    }
    console {
        facility severity;
    }
    file filename {
        facility severity;
        explicit-priority;
        match "regular-expression";
        archive {
            (binary-data| no-binary-data);
            files number;
            size maximum-file-size;
            start-time "YYYY-MM-DD.hh:mm";
            transfer-interval minutes;
            (world-readable | no-world-readable);
        }
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        allow-duplicates
        exclude-hostname
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
        match-strings [match-strings...]
        routing-instance routing-instance-name;
        source-address source-address;
        structured-data {
```

```
        brief;
      }
      port port-number;
    }
    log-rotate-frequency frequency;
    routing-instance routing-instance-name;
    server {
      routing-instances (routing-instance-name | all | default) {
        disable;
    source-address source-address;
    time-format(millisecond | year | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
    }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
IPv6 addresses using dedicated management instance mgmt_junos supported in Junos OS Release 18.1R1.

Description

Configure the types of system log messages to send to files, to a remote destination, to user terminals, or to the system console.

The remaining statements are explained separately.

Options

archive—Define parameters for archiving log messages. As of Junos OS 18.1R1, supports IPv6 addresses using dedicated management instance mgmt_junos.

console—Send log messages of a specified class and severity to the console.

file—Send log messages to a named file. As of Junos OS 18.1R1, supports IPv6 addresses using dedicated management instance mgmt_junos.

host —Remote location to be notified of specific log messages. As of Junos OS 18.1R1, supports IPv6 addresses using dedicated management instance mgmt_junos.

log-rotate-frequency—Configure the interval for checking logfile size and archiving messages.

server—Enable a syslog server for compute nodes and VMs in an App Engine.

source-address—Include a specified address as the source address for log messages. As of Junos OS 18.1R1, supports IPv6 addresses using dedicated management instance mgmt_junos.

time-format—Additional information to include in the system log time stamp.

user—Notify a specific user of the log event.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

System Log Explorer

system (Memory)

Syntax

```
system {
    frequency (minutes | hours | days) value;
    minor-event {
        threshold swap-usage value ;
        action snmp-trap;
    }
    major-event {
        threshold swap-usage value ;
        action [snmp-trap | live-vmcore];
    }
    critical-event {
        threshold swap-usage value ;
        action [snmp-trap | live-vmcore | (RE-restart | RE-switchover)];
    }
}
```

Hierarchy Level

```
[edit system monitor memory]
```

Release Information

Statement introduced in Junos OS Release 20.1 for MX Series and PTX Series routers.

Description

Configure system level memory monitoring.

Options

frequency— Specify the frequency of system level memory monitoring. You can specify the frequency in days, hours or minutes. Possible values: 1 through 65535.

minor-event— Indicates a non-critical event that, if left unchecked, may cause an interruption in service or degradation in performance but does not significantly affect the device.

major-event— Indicates an event that, if left unchecked, may result in significant loss of service or interruption of traffic.

critical-event— Indicates an event that, if left unchecked, may result in serious loss of service or interruption of traffic. In case a critical event is triggered, you can either restart the Routing Engine or configure the master Routing Engine to switchover gracefully to a backup Routing Engine without interruption in packet forwarding.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

System Log Explorer

time-format

Syntax

```
time-format (year | millisecond | year millisecond);
```

Hierarchy Level

```
[edit system syslog]
[edit security log]
```

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 20.2R1 for SRX Series devices.

Description

Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

However, in a Junos OS specific implementation using the FreeBSD console for a syslog destination, additional time information is available in system log messages for that destination when you configure the destination through a **host** statement.

By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, **Aug 21 12:36:30**.

The following example illustrates the format for a timestamp that includes both the millisecond (**401**) and the year (**2006**):

```
Aug 21 12:36:30.401 2006
```

However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

NOTE: When the **structured-data** statement is included at the **[edit system syslog file *filename*]** hierarchy level, this statement is ignored for the file.

Options

millisecond—Include the millisecond in the timestamp.

year—Include the year in the timestamp.

Required Privilege Level

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

RELATED DOCUMENTATION

Including the Year or Millisecond in Timestamps | 1496

structured-data | 2509

trace

Syntax

```
trace application {
    application-name {
        node {
            node-name {
                level level;
                group group-name {
                    enabled (off | on);
                    tracepoint tracepoint-name {
                        enabled (off | on);
                    }
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Evolved 18.2R1.

Description

Set system-wide tracing options for Junos OS Evolved. Tracing is a process about getting information regarding a program's execution. A programmer adds specific code to a program, called a *tracepoint*, which when enabled triggers a log event, which gives the programmer visibility into how the program is executing.

Options

application-name—Name of the application for which tracing should be applied. You can see a list of the applications for Junos OS Evolved by issuing the **show system applications** command. If you want to enable tracing for all applications, use the value **all**.

enabled (on | off)—Enter **on** to enable or **off** to to disable. This option has two locations in the hierarchy, one for enabling or disabling an entire group, and one for enabling or disabling specific tracepoints.

group *group-name*—The name of the trace group for which the configuration should be applied.

level *level*—Trace level of the application. The following levels are available, listed in the order of highest severity first:

- emergency—Trace emergency messages (system is unusable).
- alert—Trace alert messages (take immediate action).
- critical—Trace critical conditions.
- error—Trace error conditions.
- warning—Trace warning conditions.
- notice—Trace normal but significant conditions.
- info—Trace informational messages.
- debug—Trace debug messages.

You can configure the application's level here. The program determines the level of the tracepoints. If the application's level is at least as inclusive as (that is, the same as or of higher severity) the tracepoint's level, then the trace event is able to fire. If the application's level is less inclusive (of lower severity) than the tracepoint's level, then the trace event is not able to fire.

The default trace level is **info**.

node *node-name*—Name of a node. Node names can be **re0**, **re1**, **fpc0**, **fpc1**, and so on, depending on the system.

tracepoint *tracepoint-name*—Name of a tracepoint. A tracepoint is an event in the program, which can give the developer visibility into how the program is executing.

Required Privilege Level
admin

traceoptions (Security Log)

Syntax

```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag (all | configuration | hpl | report | source);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement modified in Junos OS Release 9.2.
The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Configure security log tracing options.

Options

- **file**—Configure the trace file 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, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

Default: 10 files

- **match *regular-expression***—Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When 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 a filename.

  Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

  Range: 10 KB through 1 GB

  Default: 128 KB
- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **configuration**—Trace configuration events
  - **hpl**— Trace HPL logging
  - **report**— Trace report
  - **source**—Communicate with security log forwarder
- **no-remote-trace**—Set remote tracing as disabled.

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

RELATED DOCUMENTATION

syslog (System) | **2510**

traceoptions (System)

Syntax

```
traceoptions {
    file {
        files files;
        size size;
    }
    level [ all | debug | info| warning| error | critical ];
}
```

Hierarchy Level

```
[edit system monitor]
```

Release Information

Statement introduced in Junos OS Release 20.2R1 for MX Series and PTX Series routers.

Description

Configure the system memory monitoring trace options on your PTX and MX Series routers. The memory monitoring system on your device monitors anomalies with respect to the memory utilization of Junos applications and overall system in the control plane of your device. Apart from monitoring the system memory, you can also configure the device to monitor the per-process memory footprint as well to help detect possible leaks and take configured action.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. The files are available at the **/var/log/jsysmon.log** .

files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1000 files

Default: 10 files

Level—Specify the level for trace logging.

all—Trace all messages.

critical—Trace critical messages.

debug—Trace debug messages.

error—Trace error messages.

info—Trace information messages.

warning—Trace warning messages.

Default: error

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. Note that if you specify a maximum file size, you also must specify a maximum number of trace files with the files option.

Syntax: xk to specify KB, xm to specify MB, and xg to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 128 KB

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS System Log Overview | **1467**

tracing

Syntax

```
tracing {
    destination-override syslog host ip-address;
}
```

Hierarchy Level

```
[edit system]
```

Release Information
Statement introduced in Junos OS Release 9.2.

Description
Configure the router to enable remote tracing to a specified host IP address. The default setting is disabled.

The following processes are supported:

- chassisd—Chassis-control process
- eventd—Event-processing process
- cosd—Class-of-service process
- spd—Adaptive-services process

You can use the **no-remote-trace** statement, under the **[edit system process-name traceoptions]** hierarchy, to disable remote tracing.

Options
destination-override syslog host *ip-address*—Overrides the global config under **system tracing** and has no effect if **system tracing** is not configured.

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

RELATED DOCUMENTATION

Junos OS Tracing and Logging Operations

destination-override | 2449

no-remote-trace

transport (Security Log)

Syntax

```
transport {
    protocol (udp | tcp | tls);
    tls-profile tls-profile-name;
    tcp-connections tcp-connections;
}
```

Hierarchy Level

```
[edit security log]
[edit logical-systems name security log]
[edit tenants tenant-name security log]
```

Release Information

Statement introduced in Junos OS Release 12.1X46-D25.
The [edit **logical-systems** *name* security log] and [edit **tenants** *tenant-name* security log] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Configure security log transport options.

Options

protocol—Specify the type of transport protocol to be used to log the data.

- **UDP**—Set the transport protocol to UDP.
- **TCP**—Set the transport protocol to TCP.
- **TLS**—Set the transport protocol to TLS.

Default: UDP.

tls-profile *tls-profile-name*—Specify the TLS profile name.

tcp-connections *tcp-connections*—Specify the number of TCP connections per SPU.

Range: 1 through 5.

Default: 1.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding AppTrack

ukern-trace

Syntax

```
ukern-trace {
   log {
      app-type dfw;
      logging (off | on);
   }
}
```

Hierarchy Level

```
[edit chassis fpc ],
[edit chassis lcc name fpc ],
[edit chassis member name fpc ]
```

Release Information
Statement introduced in Junos OS Release 17.4

Description
Enable or disable logging of all debugging firewall (DFW) ukern-trace logs on the specified FPC slot. The CLI change takes effect immediately and persists after the FPC slot reboots.

Options
app-type—Name of application with ukern-trace logs. The only supported app-type is dfw.

logging—Turn ukern-trace logging on or off. By default logging is on.

Required Privilege Level
interface

RELATED DOCUMENTATION

Junos OS System Log Overview | 1467

user (System Logging)

Syntax

```
user (username | *) {
    facility severity;
    match "regular-expression";
    match-strings string-name;
}
```

Hierarchy Level

```
[edit system syslog]
```

Release Information

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

Description

Configure the logging of system messages to user terminals.

Options

* (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.

facility—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Table 147 on page 1470.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 148 on page 1471.

username—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one **user** statement.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Directing System Log Messages to a User Terminal | 1531

Junos OS System Logging Facilities and Message Severity Levels | 1470

world-readable

Syntax

```
world-readable | no-world-readable;
```

Hierarchy Level

[edit system **syslog archive**],
[edit system **syslog file** *filename* **archive**]

Release Information

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

Description

Grant all users permission to read log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default

no-world-readable

Required Privilege Level

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

RELATED DOCUMENTATION

Specifying Log File Size, Number, and Archiving Properties | 1490

CHAPTER 77

Configuration Statement: App-Engine

IN THIS CHAPTER

- routing-instance | 2529

routing-instance

Syntax

```
routing-instance routing-instance-name{
    family inet {
        address ip-address;
    }
}
```

Hierarchy Level

```
[edit services app-engine compute-cluster compute-cluster-name local-management],
[edit services app-engine virtual-machines instance instance-name local-management]
```

Release Information

Statement introduced in Junos OS Release 13.2.

Description

(Optional) Configure a routing instance for the JunosV App Engine infrastructure. Packets are restricted to the specified routing instance. By specifying the routing instance, the JunosV App Engine infrastructure can be made to operate in a non-default routing instance. This feature ensures that JunosV App Engine traffic can be segregated from other traffic.

If the **routing-instance** statement is absent from the **[edit services app-engine virtual-machines instance *instance-name* local-management]** hierarchy level, the virtual machine (VM) will inherit this routing instance from its **[edit services app-engine compute-cluster *compute-cluster-name* local-management]** hierarchy level.

> **NOTE:** Additional configuration under the **[edit routing-instances]** hierarchy level is required to ensure that the Routing Engine interface address belongs to that particular routing instance on the routing engine. Each routing instance consists of sets of the following: Routing tables, interfaces that belong to these routing tables (optional, depending upon the routing instance type), and routing option configurations.

Options

routing-instance-name—Name of the routing instance.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

PART 14

Operational Commands

Operational Commands: General | **2532**

Operational Commands: Realtime Performance Monitoring | **2593**

Operational Commands: Analyzers and Port Mirroring | **2615**

Operational Commands: sFlow Monitoring Technology | **2618**

Operational Commands: Ethernet OAM Connectivity Fault Management | **2632**

Operational Commands: Ethernet OAM Link Fault Management | **2814**

Operational Commands: Uplink Failure Detection | **2834**

Operational Commands: RPM | **2837**

Operational Commands: SNMP | **2859**

Operational Commands: Port Mirroring | **2916**

Operational Commands: System Logging | **2919**

Monitoring Operational Commands | **2960**

CHAPTER 78

Operational Commands: General

IN THIS CHAPTER

- monitor traffic | **2533**
- ping | **2549**
- request system debug-info | **2557**
- show pfe statistics bridge | **2561**
- show pfe data | **2567**
- show system errors | **2579**
- show system errors history | **2583**
- traceroute | **2586**

monitor traffic

Syntax

```
monitor traffic
<brief | detail | extensive>
<absolute-sequence>
<count count>
<interface interface-name>
<layer2-headers>
<matching matching>
<no-domain-names>
<no-promiscuous>
<no-resolve>
<no-timestamp>
<print-ascii>
<print-hex>
<read-file filename>
<resolve-timeout>
<size size>
<write-file filename>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Options **read-file** and **write-file** introduced in Junos OS Release 19.1R1.

Description

Display packet headers or packets received and sent from the Routing Engine.

NOTE:

- Using the **monitor-traffic** command can degrade router or switch performance.
- Delays from DNS resolution can be eliminated by using the **no-resolve** option.

NOTE: This command is not supported on the QFabric system.

> **NOTE:** In Junos OS Evolved, if you modify an interface that you are monitoring with the **monitor traffic interface** command, the monitoring session ends with the message: pcap_loop: read: Device not configured. To continue monitoring the interface, rerun the **monitor traffic interface** command. However, if the monitored interface is removed, the command session continues, but there will be no packets or errors reported.

Options

none—(Optional) Display packet headers transmitted through fxp0. On a TX Matrix Plus router, display packet headers transmitted through em0.

brief | detail | extensive—(Optional) Display the specified level of output.

absolute-sequence—(Optional) Display absolute TCP sequence numbers.

count *count*—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The monitor traffic command quits automatically after displaying the number of packets specified.

interface *interface-name*—(Optional) Specify the interface on which the **monitor traffic** command displays packet data. If no interface is specified, the **monitor traffic** command displays packet data arriving on the lowest-numbered interface.

layer2-headers—(Optional) Display the link-level header on each line.

matching *matching*—(Optional) Display packet headers that match a regular expression. Use matching expressions to define the level of detail with which the **monitor traffic** command filters and displays packet data.

no-domain-names—(Optional) Suppress the display of the domain portion of hostnames. With the **no-domain-names** option enabled, the **monitor traffic** command displays only **team** for the hostname **team.company.net**.

no-promiscuous—(Optional) Do not put the interface into promiscuous mode.

no-resolve—(Optional) Suppress reverse lookup of the IP addresses.

no-timestamp—(Optional) Suppress timestamps on displayed packets.

print-ascii—(Optional) Display each packet in ASCII format.

print-hex—(Optional) Display each packet, except the link-level header, in hexadecimal format.

read-file *filename*—Read packets from the file specified.

resolve-timeout *timeout*—(Optional) Amount of time the router or switch waits for each reverse lookup before timing out. You can set the timeout for 1 through 4,294,967,295 seconds. The default is 4 seconds. To display each packet, use the **print-ascii**, **print-hex**, or **extensive** option.

size *size*—(Optional) Read but do not display up to the specified number of bytes for each packet. When set to **brief** output, the default packet size is 96 bytes and is adequate for capturing IP, ICMP, UDP, and TCP packet data. When set to **detail** and **extensive** output, the default packet size is 1514. The **monitor traffic** command truncates displayed packets if the matched data exceeds the configured size.

write-file *filename*—Write packets to the file specified.

Additional Information

In the **monitor traffic** command, you can specify an expression to match by using the **matching** option and including the expression in quotation marks:

```
monitor traffic matching "expression"
```

Replace ***expression*** with one or more of the match conditions listed in Table 209 on page 2535.

Table 209: Match Conditions for the monitor traffic Command

Match Type	Condition	Description
Entity	**host [*address* | *hostname*]**	Matches packets that contain the specified address or hostname. The protocol match conditions **arp**, **ip**, or **rarp**, or any of the directional match conditions can be prepended to the **host** match condition.
	net *address*	Matches packets with source or destination addresses containing the specified network address.
	net *address* mask *mask*	Matches packets containing the specified network address and subnet mask.
	port (*port-number* | *port-name*)	Matches packets containing the specified source or destination TCP or UDP port number or port name. In place of the numeric port address, you can specify a text synonym, such as **bgp** (179), **dhcp** (67), or **domain** (53) (the port numbers are also listed).

Table 209: Match Conditions for the monitor traffic Command *(continued)*

Match Type	Condition	Description
Directional	**dst**	Matches packets going to the specified destination. This match condition can be prepended to any of the entity type match conditions.
	src	Matches packets from a specified source. This match condition can be prepended to any of the entity type match conditions.
	src and **dst**	Matches packets that contain the specified source and destination addresses. This match condition can be prepended to any of the entity type match conditions.
	src or **dst**	Matches packets containing either of the specified addresses. This match condition can be prepended to any of the entity type match conditions.
Packet Length	**less *value***	Matches packets shorter than or equal to the specified value, in bytes.
	greater *value*	Matches packets longer than or equal to the specified value, in bytes.

Table 209: Match Conditions for the monitor traffic Command *(continued)*

Match Type	Condition	Description
Protocol	**amt**	Matches all AMT packets. Use the extensive level of output to decode the inner IGMP packets in addition to the AMT outer packet.
	arp	Matches all ARP packets.
	ether	Matches all Ethernet packets.
	ether (broadcast | multicast)	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with**src** and **dst**.
	ether *protocol* (*address* | (arp | ip | rarp))	Matches packets with the specified Ethernet address or Ethernet packets of the specified protocol type. The **ether protocol** arguments **arp**, **ip**, and **rarp** are also independent match conditions, so they must be preceded by a backslash (\) when used in the **ether protocol** match condition.
	icmp	Matches all ICMP packets.
	ip	Matches all IP packets.
	ip (broadcast | multicast)	Matches broadcast or multicast IP packets.
	ip protocol (*address* | (icmp | igrp | tcp | udp))	Matches packets with the specified address or protocol type. The **ip protocol** arguments **icmp**, **tcp**, and **udp** are also independent match conditions, so they must be preceded by a backslash (\) when used in the **ip protocol** match condition.
	isis	Matches all IS-IS routing messages.
	proto *ip-protocol-number*	Matches packets whose headers contain the specified IP protocol number.
	rarp	Matches all RARP packets.

Table 209: Match Conditions for the monitor traffic Command *(continued)*

Match Type	Condition	Description
	tcp	Matches all TCP datagrams.
	udp	Matches all UDP datagrams.

To combine expressions, use the logical operators listed in Table 210 on page 2538.

Table 210: Logical Operators for the monitor traffic Command

Logical Operator (Highest to Lowest Precedence)	Description
!	Logical NOT. If the first condition does not match, the next condition is evaluated.
&&	Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.
||	Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.
( )	Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).

You can use relational operators to compare arithmetic expressions composed of integer constants, binary operators, a length operator, and special packet data accessors. The arithmetic expression matching condition uses the following syntax:

```
monitor traffic matching "ether[0] & 1 != 0""arithmetic_expression relational_operator arithmetic_expression"
```

The packet data accessor uses the following syntax:

```
protocol [byte-offset <size>]
```

The optional *size* field represents the number of bytes examined in the packet header. The available values are**1**, **2**, or **4** bytes. The following sample command captures all multicast traffic:

```
user@host> monitor traffic matching "ether[0] & 1 != 0"
```

To specify match conditions that have a numeric value, use the arithmetic and relational operators listed in Table 211 on page 2539.

NOTE: Because the Packet Forwarding Engine removes Layer 2 header information before sending packets to the Routing Engine:

- The **monitor traffic** command cannot apply match conditions to inbound traffic.
- The **monitor traffic interface** command also cannot apply match conditions for Layer 3 and Layer 4 packet data, resulting in the **match** pipe option (**| match**) for this command for Layer 3 and Layer 4 packets not working either. Therefore, ensure that you specify match conditions as described in this command summary. For more information about match conditions, see Table 209 on page 2535.
- The 802.1Q VLAN tag information included in the Layer 2 header is removed from all inbound traffic packets. Because the **monitor traffic interface ae[*x*]** command for aggregated Ethernet interfaces (such as) only shows inbound traffic data, the command does not show VLAN tag information in the output.

Table 211: Arithmetic and Relational Operators for the monitor traffic Command

Arithmetic or Relational Operator	Description
Arithmetic Operator	
+	Addition operator.
-	Subtraction operator.
/	Division operator.
&	Bitwise AND.
*	Bitwise exclusive OR.
|	Bitwise inclusive OR.
Relational Operator (Highest to Lowest Precedence)	
<=	If the first expression is less than or equal to the second, the packet matches.

Table 211: Arithmetic and Relational Operators for the monitor traffic Command *(continued)*

Arithmetic or Relational Operator	Description
>=	If the first expression is greater than or equal to the second, the packet matches.
<	If the first expression is less than the second, the packet matches.
>	If the first expression is greater than the second, the packet matches.
=	If the compared expressions are equal, the packet matches.
!=	If the compared expressions are unequal, the packet matches.

Required Privilege Level

trace

maintenance

List of Sample Output

monitor traffic count on page 2541
monitor traffic detail count on page 2541
monitor traffic extensive (Absolute Sequence) on page 2541
monitor traffic extensive (Relative Sequence) on page 2542
monitor traffic extensive count on page 2542
monitor traffic interface on page 2542
monitor traffic matching on page 2543
monitor traffic (TX Matrix Plus Router) on page 2543
monitor traffic (QFX3500 Switch) on page 2545
monitor traffic matching icmp on page 2545
monitor traffic matching IP protocol number on page 2546
monitor traffic matching arp on page 2547
monitor traffic matching port on page 2547
monitor traffic read-files on page 2548
monitor traffic write-file on page 2548

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

monitor traffic count

user@host> **monitor traffic count 2**

```
listening on fxp0
04:35:49.814125  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529478 win 16798 (DF)
04:35:49.814185
Out my-server.work.net.telnet > my-server.home.net.1295: P
1:38(37) ack 0 win 17680 (DF) [tos 0x10]
```

monitor traffic detail count

user@host> **monitor traffic detail count 2**

```
listening on fxp0
04:38:16.265864  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529971 win 17678 (DF) (ttl 121, id 6812)
04:38:16.265926
Out my-server.work.net.telnet.telnet > my-server.home.net.1295: P 1:38(37) ack 0
win 17680 (DF) [tos 0x10]  (ttl 6)
```

monitor traffic extensive (Absolute Sequence)

user@host> **monitor traffic extensive no-domain-names no-resolve no-timestamp count 20 matching "tcp" absolute-sequence**

```
listening on fxp0
 In 203.0.113.193.179 > 192.168.4.227.1024: . 4042780859:4042780859(0)
ack 1845421797 win 16384 <nop,nop,timestamp 4935628 965951> [tos 0xc0]  (ttl )
 In 203.0.113.193.179 > 192.168.4.227.1024: P 4042780859:4042780912(53)
ack 1845421797 win 16384
<nop,nop,timestamp 4935628 965951>:
BGP [|BGP UPDAT)
In 192.168.4.227.1024 > 203.0.113.193.179:
P 1845421797:1845421852(55) ack 4042780912 win 16384 <nop,nop,timestamp 965951
4935628>: BGP [|BGP UPDAT)
...
```

monitor traffic extensive (Relative Sequence)

`user@host>` **monitor traffic extensive no-domain-names no-resolve no-timestamp count 20 matching "tcp"**

```
listening on fxp0
 In 172.24.248.221.1680 > 192.168.4.210.23: . 396159737:396159737(0)
ack 1664980689 win 17574 (DF) (ttl 121, id 50003)
Out 192.168.4.210.23 > 172.24.248.221.1680: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]  (ttl 64, id 5394)
 In 203.0.113.193.179 > 192.168.4.227.1024: P 4042775817:4042775874(57)
ack 1845416593 win 16384 <nop,nop,timestamp 4935379 965690>: BGP [|BGP UPDAT)
...
```

monitor traffic extensive count

monitor traffic extensive count 5 no-domain-names no-resolve

```
listening on fxp013:18:17.406933
In 192.168.4.206.2723610880 > 172.17.28.8.2049:
40 null (ttl 64, id 38367)13:18:17.407577
In 172.17.28.8.2049 > 192.168.4.206.2723610880:
reply ok 28 null (ttl 61, id 35495)13:18:17.541140
In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
0000 0100 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 000013:18:17.591513
In 172.24.248.156.4139 > 192.168.4.210.23:
3556964918:3556964918(0)
ack 295526518 win 17601 (DF)
(ttl 121, id 14)13:18:17.591568
Out 192.168.4.210.23 >
172.24.248.156.4139: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]
(ttl 64, id 52376)
```

monitor traffic interface

`user@host>` **monitor traffic interface fxp0**

```
listening on fxp0.0
18:17:28.800650  In server.home.net.723 > host1-0.lab.home.net.log
18:17:28.800733 Out host2-0.lab.home.net.login > server.home.net.7
18:17:28.817813  In host30.lab.home.net.syslog > host40.home0
18:17:28.817846  In host30.lab.home.net.syslog > host40.home0
...
```

monitor traffic matching

`user@host>` **monitor traffic matching "net 192.168.1.0/24"**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes

Reverse lookup for 192.168.1.255 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use no-resolve to avoid reverse lookups on IP addresses.

21:55:54.003511  In IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003585 Out IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003864  In arp who-has 192.168.1.17 tell 192.168.1.9
...
```

monitor traffic (TX Matrix Plus Router)

`user@host>` **monitor traffic**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em0, capture size 96 bytes
04:11:59.862121 Out IP truncated-ip - 25 bytes missing!
summit-em0.example.net.syslog > sv-log-01.example.net.syslog:
SYSLOG kernel.info, length: 57
04:11:59.862303
Out IP truncated-ip - 25 bytes missing!
summit-em0.example.net.syslog >
sv-log-02.example.net.syslog: SYSLOG kernel.info, length: 57
04:11:59.923948
```

```
In IP aj-em0.example.net.65235 >
summit-em0.example.net.telnet: .
ack 1087492766 win 33304 <nop,nop,timestamp 42366734 993490>
04:11:59.923983 Out IP truncated-ip - 232 bytes missing!
summit-em0.example.net.telnet > aj-em0.example.net.65235: P 1:241(240) ack 0 win
33304
<nop,nop,timestamp 993590 42366734>
04:12:00.022900
In IP aj-em0.exmaple.net.65235 >
summit-em0.example.net.telnet: . ack 241 win 33304 <nop,nop,timestamp 42366834
993590>
04:12:00.141204
In IP truncated-ip - 40 bytes missing!
ipg-lnx-shell1.example.net.46182 > summit-em0.example.net.telnet: P
2950530356:2950530404(48) ack 485494987 win 63712
<nop,nop,timestamp 1308555294 987086>
04:12:00.141345
Out IP summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 1:6(5)
ack 48 win 33304
<nop,nop,timestamp 993809 1308555294>
04:12:00.141572
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.example.net.telnet: .
ack 6 win 63712
<nop,nop,timestamp 1308555294 993809>
04:12:00.141597
Out IP summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 6:10(4) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.141821
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.exmaple.net.telnet: .
ack 10 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.141837 Out IP truncated-ip - 2 bytes missing!
summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 10:20(10) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.142072
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.example.net.telnet: . ack 20 win 63712
<nop,nop,timestamp 1308555294 993810>
04:12:00.142089 Out IP summit-em0.example.net.telnet >
```

```
ipg-lnx-shell1.example.net.46182: P 20:28(8) ack 48 win 33304 <nop,nop,timestamp
993810 1308555294>
04:12:00.142321
In IP ipg-lnx-shell1.exmample.net.46182 >
summit-em0.englab.example.net.telnet: .
ack 28 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.142337
Out IP truncated-ip - 1 bytes missing!
summit-em0.example.net.telnet >
ipg-lnx-shell.example.net.46182: P 28:37(9) ack 48 win 33304 <nop,nop,timestamp
993810 1308555294>
...
```

monitor traffic (QFX3500 Switch)

`user@switch>` **monitor traffic**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on me4, capture size 96 bytes
Reverse lookup for 172.22.16.246 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.
16:35:32.240873 Out IP truncated-ip - 112 bytes missing! labqfx-me0.example.net.ssh
 >
172.22.16.246.telefinder: P 4200727624:4200727756(132) ack 2889954831 win 65535
16:35:32.240900 Out IP truncated-ip - 176 bytes missing! labqfx-me0.example.net.ssh
 >
172.22.16.246.telefinder: P 132:328(196) ack 1 win 65535
...
```

monitor traffic matching icmp

`user@host>` **monitor traffic matching "icmp" no-resolve**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

09:23:17.728737  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
322, length 40
09:23:17.728780 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq 322,
```

```
 length 40
09:23:18.735848  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
323, length 40
09:23:18.735891 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq 323,
 length 40
09:23:19.749732  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
324, length 40
09:23:19.749775 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq 324,
 length 40
09:23:20.749747  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
325, length 40
09:23:20.749791 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq 325,
 length 40
...
```

monitor traffic matching IP protocol number

`user@host>` **monitor traffic matching "proto 89" no-resolve**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

13:06:14.700311  In IP truncated-ip - 16 bytes missing! 10.94.211.254 > 224.0.0.
5: OSPFv2, Hello, length 56
13:06:16.067010  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:16.287566  In IP truncated-ip - 20 bytes missing! 10.94.211.142 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:20.758500  In IP truncated-ip - 16 bytes missing! 10.200.211.254 > 224.0.0
.5: OSPFv2, Hello, length 56
13:06:24.309882  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:24.396699  In IP truncated-ip - 16 bytes missing! 10.94.211.254 > 224.0.0.
5: OSPFv2, Hello, length 56
13:06:25.067386  In IP truncated-ip - 20 bytes missing! 10.94.211.142 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:29.499988  In IP truncated-ip - 16 bytes missing! 10.200.211.254 > 224.0.0
.5: OSPFv2, Hello, length 56
13:06:32.858753  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
...
```

monitor traffic matching arp

user@host> **monitor traffic matching “arp” no-resolve**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

11:57:54.664501  In arp who-has 10.10.213.109 (00:1f:d5:f3:28:30) tell 10.10.213.31
11:57:56.828387  In arp who-has 10.10.213.233 (00:24:9d:06:77:4f) tell 10.10.213.31
11:58:01.735803  In arp who-has 10.10.213.251 (88:e0:f4:1d:41:40) tell 10.10.213.31
11:58:04.663241  In arp who-has 10.10.213.254 tell 10.94.211.170
11:58:28.488191  In arp who-has 10.10.213.149 (00:e0:91:c2:ff:8d) tell 10.10.213.31
11:58:41.858612  In arp who-has 10.10.213.148 tell 10.94.211.254
11:58:42.621533  In arp who-has 10.10.213.254 (5f:5e:ac:79:49:81) tell 10.10.213.31
11:58:44.533391  In arp who-has 10.10.213.186 tell 10.94.211.254
11:58:45.170405  In arp who-has 10.10.213.186 tell 10.94.211.254
11:58:45.770512  In arp who-has 10.10.213.186 tell 10.94.211.254
```

monitor traffic matching port

user@host> **monitor traffic matching “port 22” no-resolve**

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

13:14:19.108089  In IP 192.0.2.22.56714 > 10.19.300.05.22: S
2210742342:2210742342(0) win 65535 <mss 1360,nop,wscale 7,nop,nop,sackOK>
13:14:19.108165 Out IP 10.19.300.05.22 > 192.0.2.22.56714: S 23075150:23075150(0)
 ack 2210742343 win 65535 <mss 1460,nop,wscale 1,sackOK,eol>
13:14:19.136883  In IP 192.0.2.22.56714 > 10.19.300.05.22: . ack 1 win 32768
13:14:19.231364 Out IP truncated-ip - 1 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 1:22(21) ack 1 win 33320
13:14:19.260174  In IP truncated-ip - 10 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 1:31(30) ack 22 win 32767
13:14:19.284865 Out IP truncated-ip - 964 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 22:1006(984) ack 31 win 33320
13:14:19.314549  In IP truncated-ip - 652 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 31:703(672) ack 1006 win 32760
13:14:19.414135 Out IP 10.19.300.05.22 > 192.0.2.22.56714: . ack 703 win 33320
13:14:19.443858  In IP 192.0.2.22.56714 > 10.19.300.05.22: P 703:719(16) ack 1006
 win 32760
13:14:19.467379 Out IP truncated-ip - 516 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 1006:1542(536) ack 719 win 33320
```

```
13:14:19.734097  In IP 192.0.2.22.56714 > 10.19.300.05.22: . ack 1542 win 32768
13:14:19.843574  In IP truncated-ip - 508 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 719:1247(528) ack 1542 win 32768
...
```

monitor traffic read-files

`user@host>` **monitor traffic read-file tcpdump_20_7_18.pcap**

```
15:20:42.597413 Out IP 128.0.0.1.6234 > 128.0.0.17.37217: . ack 1416364513 win
65535 <nop,nop,timestamp 2494269906 347794433>
15:20:42.597424 Out IP 128.0.0.1.6234 > 128.0.0.16.49400: . ack 3549610340 win
65535 <nop,nop,timestamp 2494269906 347799892>
15:20:42.598214 Out IP truncated-ip - 32 bytes missing! 128.0.0.1.6234 >
128.0.0.16.49400: P 0:40(40) ack 1 win 65535 <nop,nop,timestamp 2494269907
347799892>
                         0001 0000 0020 0000
```

monitor traffic write-file

`user@host>` **monitor traffic write-file *filename***

```
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em1, capture size 96 bytes

^C
955 packets received by filter
0 packets dropped by kernel
```

ping

List of Syntax

Syntax on page 2549
Syntax (QFX Series) on page 2549
Syntax (Junos OS Evolved) on page 2550

Syntax

```
ping host
<bypass-routing>
<ce-ip destination-ip-address instance routing-instance-name source-ip source-ip-address>
<count requests>
<do-not-fragment>
<inet | inet6>
<interface source-interface>
<interval seconds>
<no-resolve>
<pattern string>
<rapid>
<record-route>
<routing-instance routing-instance-name>
<logical-system logical-system-name>
<tenant tenant-name>
<size bytes>
<source source-address>
<tos type-of-service>
<ttl value>
<verbose>
<wait seconds>
```

Syntax (QFX Series)

```
ping host
<bypass-routing>
<count requests>
<detail>
<do-not-fragment>
<inet>
<interface source-interface>
<interval seconds>
<logical-system logical-system-name>
<loose-source value>
<mac-address mac-address>
```

```
<no-resolve>
<pattern string>
<rapid>
<record-route>
<routing-instance routing-instance-name>
<size bytes>
<source source-address>
<strict>
< strict-source value>
<tos type-of-service>
<ttl value>
<verbose>
<wait seconds>
```

Syntax (Junos OS Evolved)

```
ping host
<bypass-routing>
<ce-ip destination-ip-address instance routing-instance-name source-ip source-ip-address>
<count requests>
<do-not-fragment>
<inet | inet6>
<interface source-interface>
<interval seconds>
<no-resolve>
<pattern string>
<rapid>
<record-route>
<routing-instance routing-instance-name>
<size bytes>
<source source-address>
<tos type-of-service>
<ttl value>
<verbose>
<wait seconds>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
ce-ip option introduced in Junos OS Release 17.3 for MX Series routers with MPC and MIC interfaces.

The following options are deprecated for Junos OS Evolved Release 18.3R1: **detail**, **logical-system**, **loose-source**, **mac-address**, **strict**, **strict-source**, and **vpls**.
The command **tenant** option is introduced in Junos OS Release 19.2R1 for SRX Series.

Description

Check host reachability and network connectivity. The **ping** command sends Internet Control Message Protocol (ICMP) ECHO_REQUEST messages to elicit ICMP ECHO_RESPONSE messages from the specified host. Press Ctrl+c to interrupt a ping command.

Options

host—IP address or hostname of the remote system to ping.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

ce-ip *destination-ip-address* instance *routing-instance-name* source-ip *source-ip-address*—(MX Series routers with MPC and MIC interfaces only) (Optional) Check the connectivity information of customer edge (CE) devices, such as reachability, attachment points, and MAC addresses, from a provider edge (PE) device in a virtual private LAN service (VPLS), hierarchical VPLS (H-VPLS), and Ethernet VPN (EVPN) network. The **ce-ip** option is based on the LSP ping infrastructure, where the **ping** utility is extended to use the CE device IP address as the target host and the PE device loopback address as the source for a specific VPLS or EVPN routing instance.

destination-ip-address—IPv4 address of the CE device to ping.

instance *routing-instance-name*—Name of the VPLS or EVPN routing instance. The command output displays the connectivity information of the CE device based on the configured routing instance type.

source-ip *source-ip-address*—Loopback address of the PE device.

count *requests*—(Optional) Number of ping requests to send. The range of values is **1** through **2,000,000,000**. The default value is an unlimited number of requests.

detail—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Include in the output the interface on which the ping reply was received.

do-not-fragment—(Optional) Set the do-not-fragment (DF) flag in the IP header of the ping packets.

For Junos OS Evolved Release 18.3R1, IPv6 **ping** does not have **do-not-fragment** support. The **ping** command is identified as IPv6 Ping when destination is IPv6 address or **inet6** option is used.

For Junos OS IPv6 packets, this option disables fragmentation.

NOTE: In Junos OS Release 11.1 and later, when issuing the **ping** command for an IPv6 route with the **do-not-fragment** option, the maximum ping packet size is calculated by subtracting 48 bytes (40 bytes for the IPV6 header and 8 bytes for the ICMP header) from the MTU. Therefore, if the ping packet size (including the 48-byte header) is greater than the MTU, the ping operation might fail.

inet—(Optional) Ping Packet Forwarding Engine IPv4 routes.

inet6—(Optional) Ping Packet Forwarding Engine IPv6 routes.

interface *source-interface*—(Optional) Interface to use to send the ping requests.

interval *seconds*—(Optional) How often to send ping requests. The range of values, in seconds, is **1** through infinity. The default value is **1**.

logical-system *logical-system-name*—(Optional) Name of logical system from which to send the ping requests.

Alternatively, enter the **set cli logical-system *logical-system-name*** command and then run the **ping** command. To return to the main router or switch, enter the **clear cli logical-system** command.

tenant *tenant-name*—(Optional) Name of tenant system from which to send the ping requests.

loose-source *value*—(Optional) Intermediate loose source route entry (IPv4). Open a set of values.

mac-address *mac-address*—(Optional) Ping the physical or hardware address of the remote system you are trying to reach.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

pattern *string*—(Optional) Specify a hexadecimal fill pattern to include in the ping packet.

rapid—(Optional) Send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the **count** option.

record-route—(Optional) Record and report the packet's path (IPv4).

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the ping attempt. For Junos OS Evolved, the **routing-instance** option supports only **mgmt_junos**.

size *bytes*—(Optional) Size of ping request packets. The range of values, in bytes, is **0** through **65,468**. The default value is **56**, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.

source *source-address*—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

strict—(Optional) Use the strict source route option (IPv4).

strict-source *value*—(Optional) Intermediate strict source route entry (IPv4). Open a set of values.

tos *type-of-service*—(Optional) Set the type-of-service (ToS) field in the IP header of the ping packets. The range of values is **0** through **255**.

If the device configuration includes the **dscp-code-point *value*** statement at the **[edit class-of-service host-outbound-traffic]** hierarchy level, the configured DSCP value overrides the value specified in this command option. In this case, the ToS field of ICMP echo request packets sent on behalf of this command carries the DSCP value specified in the **dscp-code-point** configuration statement instead of the value you specify in this command option.

ttl *value*—(Optional) Time-to-live (TTL) value to include in the ping request (IPv6). The range of values is **0** through **255**.

verbose—(Optional) Display detailed output.

vpls *instance-name*—(Optional) Ping the instance to which this VPLS belongs.

wait *seconds*—(Optional) Maximum wait time, in seconds, after the final packet is sent. If this option is not specified, the default delay is **10** seconds. If this option is used without the count option, a default count of **5** packets is used.

Required Privilege Level
network

RELATED DOCUMENTATION

Rate Limit ICMPv4 and ICMPv6 Traffic

Pinging Customer Edge Device IP Address

List of Sample Output

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (EVPN) on page 2554
ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (VPLS) on page 2554
ping hostname on page 2554
ping hostname rapid on page 2555
ping hostname size count on page 2555

Output Fields

When you enter this command, you are provided feedback on the status of your request. An exclamation point (**!**) indicates that an echo reply was received. A period (**.**) indicates that an echo reply was not received within the timeout period. An **x** indicates that an echo reply was received with an error code. These packets are not counted in the received packets count. They are accounted for separately.

When pinging a nonexistant route, the display output of **ping** command does not print the number of packets sent or received or the packet loss.

Sample Output

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (EVPN)

```
user@host> ping ce-ip 10.0.0.4 instance foo source-ip 127.0.0.1
```

```
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
--- ce-ip ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (VPLS)

```
user@host> ping ce-ip 10.0.0.4 instance foo source-ip 127.0.0.1
```

```
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
--- ce-ip ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

ping hostname

```
user@host> ping device1.example.com
```

```
PING device1.example.com (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: icmp_seq=0 ttl=253 time=1.028 ms
64 bytes from 192.0.2.0: icmp_seq=1 ttl=253 time=1.053 ms
64 bytes from 192.0.2.0: icmp_seq=2 ttl=253 time=1.025 ms
64 bytes from 1192.0.2.0: icmp_seq=3 ttl=253 time=1.098 ms
64 bytes from 192.0.2.0: icmp_seq=4 ttl=253 time=1.032 ms
64 bytes from 192.0.2.0: icmp_seq=5 ttl=253 time=1.044 ms
^C [abort]
```

ping hostname rapid

```
user@host> ping device1.example.com rapid
```

```
PING device1.example.com (192.0.2.0): 56 data bytes
!!!!!
--- device1.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.956/0.974/1.025/0.026 ms
```

ping hostname size count

```
user@host> ping device1.example.com size 200 count 5
```

```
PING device1.example.com (192.0.2.0): 200 data bytes
208 bytes from 192.0.2.0: icmp_seq=0 ttl=253 time=1.759 ms
208 bytes from 192.0.2.0: icmp_seq=1 ttl=253 time=2.075 ms
208 bytes from 192.0.2.0: icmp_seq=2 ttl=253 time=1.843 ms
208 bytes from 192.0.2.0: icmp_seq=3 ttl=253 time=1.803 ms
208 bytes from 192.0.2.0: icmp_seq=4 ttl=253 time=17.898 ms

--- device1.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.759/5.075/17.898 ms
```

Output for Junos OS Evolved:

```
user@host> ping 40.0.0.2 count 20 size 500
```

```
connect: No route to host
```

Output for Junos OS:

user@host> **ping 40.0.0.2 count 20 size 500**

```
Aug 02 12:56:56 [INFO ] Step 2: Host and Transit ping has to fail
Aug 02 12:56:56 [TRACE] [R0 evo-ptx-b] [cmd] run ping 40.0.0.2 rapid count 50 size
 500
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] PING 40.0.0.2 (40.0.0.2): 500 data bytes
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] ping: sendto: No route to host
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] .ping: sendto: No route to host
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] ping: sendto: No route to host
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] .ping: .sendto: No route to host
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] ping: sendto: No route to host
ug 02 12:57:21 [TRACE] [R0 evo-ptx-b] ..
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] --- 40.0.0.2 ping statistics ---
Aug 02 12:57:21 [TRACE] [R0 evo-ptx-b] 50 packets transmitted, 0 packets received,
 100% packet loss
```

request system debug-info

Syntax

```
request system debug-info
<node node-name>
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

Description

Collect debug information from Junos OS Evolved, such as logs. Logs are stored in the **/var/tmp/debug_collector_*timestamp*** directory. You need to know the root password of the device to use this command. Enter the root password and confirm it when requested.

Options

node *node-name*—(Optional) Identifier of the node. If a value for **node** (for example, **re0**, **re1**, **fpc0**) is given, this command collects logs only from the given node. If the node option is not provided, log information is collected from all active nodes.

Additional Information

To view the **debug_collector.log** file:

1. Exit to the shell and go to the **/var/tmp/** directory.

```
root@host:~# cd /var/tmp
root@host:/var/tmp# ls
all_logs.2719  baseline-config.conf
all_logs.2767  debug_collector_2017-11-20_13_16_45.tar.gz
```

2. Uncompress the **/var/tmp/debug_collector_*timestamp*.tar.gz** file.

```
root@host:/var/tmp# tar -xf debug_collector_2017-11-20_13_16_45.tar.gz
root@host:/var/tmp# ls
all_logs.2719         debug_collector_2017-11-20_13_16_45
all_logs.2767         debug_collector_2017-11-20_13_16_45.tar.gz
baseline-config.conf
```

3. Go to the **/var/tmp/debug_collector_*timestamp*** directory.

```
root@host:/var/tmp# cd debug_collector_2017-11-20_13_16_45
root@host:/var/tmp/debug_collector_2017-11-20_13_16_45# ls
debug_collector.log
```

4. Look at the log file.

```
root@host:/var/tmp/debug_collector_2017-11-20_13_16_45# vi debug_collector.log
2017-11-20 13:16:45 INFO: debug_collector.py:704 <module>(): Running
debug_collector as user 'root' with super user privileges...
2017-11-20 13:16:45 INFO: debug_collector.py:705 <module>(): You can monitor
detailed progress using:
2017-11-20 13:16:45 INFO: debug_collector.py:706 <module>():    tail -f
/var/tmp/debug_collector_2017-11-20_13_16_45/debug_collector.log
2017-11-20 13:16:45 INFO: debug_collector.py:323 fetch_root_pswd(): Debug
collector needs to login into all nodes in the system as root user
2017-11-20 13:25:31 DEBUG: debug_collector.py:332 fetch_root_pswd(): Passwords
 matched, proceeding with debug collection...
2017-11-20 13:25:31 INFO: debug_collector.py:225 detect_res(): Detecting REs in
 the system...
2017-11-20 13:25:31 DEBUG: debug_collector.py:239 detect_res(): Into for
2017-11-20 13:25:31 DEBUG: debug_collector.py:242 detect_res(): Into m1 not None
2017-11-20 13:25:31 DEBUG: debug_collector.py:245 detect_res(): Found RE 're0'
 in /etc/hosts
2017-11-20 13:25:31 DEBUG: debug_collector.py:248 detect_res(): Into if 1
2017-11-20 13:25:31 DEBUG: debug_collector.py:239 detect_res(): Into for
2017-11-20 13:25:31 DEBUG: debug_collector.py:242 detect_res(): Into m1 not None
2017-11-20 13:25:31 DEBUG: debug_collector.py:245 detect_res(): Found RE 're1'
 in /etc/hosts
2017-11-20 13:25:31 DEBUG: debug_collector.py:261 detect_res(): Into if 4
2017-11-20 13:25:31 INFO: debug_collector.py:265 detect_res(): This RE is 're0'
2017-11-20 13:25:31 DEBUG: debug_collector.py:266 detect_res(): This RE is 're0'
 and the other RE is 're1'
2017-11-20 13:25:32 DEBUG: debug_collector.py:269 detect_res(): Other RE 're1'
 is reachable
2017-11-20 13:25:32 INFO: debug_collector.py:274 detect_res():  List of reachable
 REs: ['re0', 're1']
2017-11-20 13:25:32 INFO: debug_collector.py:293 detect_fpcs(): Detecting FPCs
 in the system, might take upto a couple of minutes...
2017-11-20 13:25:33 DEBUG: debug_collector.py:309 detect_fpcs(): FPC 'fpc0' is
 reachable
2017-11-20 13:25:36 DEBUG: debug_collector.py:312 detect_fpcs(): FPC 'fpc1' is
 not reachable
2017-11-20 13:25:39 DEBUG: debug_collector.py:312 detect_fpcs(): FPC 'fpc2' is
```

```
 not reachable
2017-11-20 13:25:40 INFO: debug_collector.py:977 <module>(): User interrupt
detected, stopping further debug collection...
2017-11-20 13:25:40 INFO: debug_collector.py:372 create_final_archive(): Creating
 archive of all logs collected...
```

Required Privilege Level
view

List of Sample Output
request system debug-info on page 2559

Sample Output

request system debug-info

`user@host>` **request system debug-info**

```
2017-11-20 13:16:45 INFO: debug_collector.py:704 <module>(): Running debug_collector
 as user 'root' with super user privileges...
2017-11-20 13:16:45 INFO: debug_collector.py:705 <module>(): You can monitor
detailed progress using:
2017-11-20 13:16:45 INFO: debug_collector.py:706 <module>():    tail -f
/var/tmp/debug_collector_2017-11-20_13_16_45/debug_collector.log
2017-11-20 13:16:45 INFO: debug_collector.py:323 fetch_root_pswd(): Debug collector
 needs to login into all nodes in the system as root user
Please enter root password:
Please re-enter the password:
2017-11-20 13:25:31 INFO: debug_collector.py:225 detect_res(): Detecting REs in
the system...
2017-11-20 13:25:31 INFO: debug_collector.py:265 detect_res(): This RE is 're0'
2017-11-20 13:25:32 INFO: debug_collector.py:274 detect_res():  List of reachable
 REs: ['re0', 're1']
2017-11-20 13:25:32 INFO: debug_collector.py:293 detect_fpcs(): Detecting FPCs in
 the system, might take upto a couple of minutes...
^C2017-11-20 13:25:40 INFO: debug_collector.py:977 <module>(): User interrupt
detected, stopping further debug collection...
2017-11-20 13:25:40 INFO: debug_collector.py:372 create_final_archive(): Creating
 archive of all logs collected...
2017-11-20 13:25:40 INFO: debug_collector.py:380 create_final_archive(): Here it
is: /var/tmp/debug_collector_2017-11-20_13_16_45.tar.gz
```

```
2017-11-20 13:25:40 INFO: debug_collector.py:389 create_final_archive(): Debug
collector run time: 0h 8m 54s
2017-11-20 13:25:40 INFO: debug_collector.py:401 cleanup_and_exit(): Over n out!
```

show pfe statistics bridge

Syntax

```
show pfe statistics bridge
<fpc slot>
```

Release Information

Command introduced in Junos OS Release 12.1 for EX Series switches.

Description

Display information about the number of packets discarded in the ingress pipeline of the Packet Forwarding Engine, packets discarded because of egress filtering or congestion filtering, number of control packets, and general counters for dropped packets. You can use this information to inform troubleshooting investigations.

Options

none—Display bridge counter statistics for all Flexible PIC Concentrator (FPC) slots.

fpc *slot*—(Optional) Display bridge counter statistics for a specific FPC slot.

Required Privilege Level

view

RELATED DOCUMENTATION

Monitoring Switch Control Traffic

List of Sample Output

show pfe statistics bridge (EX3200 and EX4200 Switches) on page 2563
show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis) on page 2563
show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis) on page 2565
show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card) on page 2565

Output Fields

Table 212 on page 2562 lists the output fields for the **show pfe statistics bridge** command. Output fields are listed in the approximate order in which they appear.

Table 212: show pfe statistics bridge Output Fields

Field Name	Field Description
Ingress Counters	Information about ingress counters: • **Received**—Number of packets received by the bridge. • **VLAN Filtered**—Number of packets discarded because of VLAN filtering. • **Security Filtered**—Number of packets discarded because of security filtering. • **Other Discards**—Number of packets dropped by the bridge for reasons other than VLAN or security filtering.
Egress Counters	Information about egress counters: • **Unicast**—Number of unicast packets transmitted. • **Multicast**—Number of multicast packets transmitted. • **Broadcast**—Number of broadcast packets transmitted. • **Egress Filtered**—Number of egress-filtered packets (regardless of port, priority, or mode). • **TailDrop**—Number of packets filtered because of egress queue congestion. • **Forward Restrict**—Number of packets filtered because of egress forward restrictions. • **Congestion Filtered**—Number of packets filtered because of transmit queue (TxQ) congestion. • **Control Packets**—Number of control packets (sent to CPU, received from CPU, and sent to analyzer).
Drop Counters	Information about drop counters: • **Drop Mode**—Count mode of the counter. • **Drop Counter**—Counter value.
General Counters	Information about general counters: • **Drop Mode**—Count mode of the counter. • **Drop Counter**—Counter value. • **Source Not Learnt**—Number of source addresses that were not learnt because of internal congestion.
MUX PFE	Information about multiplexer PFE for oversubscribed cards: • **Drop Mode**—Count mode of the counter. • **Drop Count**—Counter value.

Sample Output

show pfe statistics bridge (EX3200 and EX4200 Switches)

user@switch> **show pfe statistics bridge**

```
Slot 0

PFE:                        0          1          2
----------------------------------------------------------------
----  Ingress Counters ----
Received:                     0         52          0
VLAN Filtered:                0          0          0
Security Filtered:            0          0          0
Other Discards:               0          0          0
----  Egress Counters ----
Unicast:                      0        104         52
Multicast:                    0          0          0
Broadcast:                    0          0          0
Egress Filtered:              0          0          0
Congestion Filtered:          0          0          0
Control Packets:              5          0          0
----  General Counters ----
Drop Mode:                  0          0          0
Drop Counter:           34217      36080       6367
Source Not Learnt:          0          0          0
```

show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis)

user@switch> **show pfe statistics bridge**

```
Slot 0
PFE:                        0          1
------------------------------------------------------------------
---- Ingress Counters ----
Received:                   946         48
VLAN Filtered:                0          0
Security Filtered:            0          0
Other Discards:               0          0
---- Egress Counters ----
Unicast:                      0          0
Multicast:                    0          0
Broadcast:                    0          0
Egress Filtered:              0          0
```

```
TailDrop:                        0            0
Forward Restrict:                0            0
Congestion Filtered:             0            0
Control Packets:              4103          896
---- Drop Counters ----
Drop Mode:                 0            0
Drop Counter:          12528            2

Slot 1

PFE:                             0            1
------------------------------------------------------------------------
---- Ingress Counters ----
Received:                        0            0
VLAN Filtered:                   0            0
Security Filtered:               0            0
Other Discards:                  0            0
---- Egress Counters ----
Unicast:                         0            0
Multicast:                       0            0
Broadcast:                       0            0
Egress Filtered:                 0            0
TailDrop:                        0            0
Forward Restrict:                0            0
Congestion Filtered:             0            0
Control Packets:                 0            0
---- Drop Counters ----
Drop Mode:                       0            0
Drop Counter:                    0            0

Slot 2

PFE:                             0             1
------------------------------------------------------------------------
---- Ingress Counters ----
Received:                        0             0
VLAN Filtered:                   0             0
Security Filtered:               0             0
Other Filtered:                  0             0
---- Egress Counters ----
Unicast:                         0             0
Multicast:                       0             0
Broadcast:                       0             0
Egress Filtered:                 0             0
```

```
TailDrop:                       0            0
Forward Restrict:               0            0
Congestion Filtered:            0            0
Control Packets:                0            0
---- Drop Counters ----
Drop Mode:                      0            0
Drop Counter:                   0            0
```

show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis)

`user@switch>` **show pfe statistics bridge fpc 2**

```
Slot 2

PFE:                        0            1
------------------------------------------------------------------------
---- Ingress Counters ----
Received:                0            0
VLAN Filtered:           0            0
Security Filtered:       0            0
Other Discards:          0            0
---- Egress Counters ----
Unicast:                 0            0
Multicast:               0            0
Broadcast:               0            0
Egress Filtered:         0            0
TailDrop:                0            0
Forward Restrict:        0            0
Congestion Filtered:     0            0
Control Packets:         0            0
---- Drop Counters ----
Drop Mode:               0            0
Drop Counter:            0            0
```

show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card)

`user@switch>` **show pfe statistics bridge fpc 8**

```
Slot 8

PFE:                         0          1          2          3
------------------------------------------------------------------------
----  Ingress Counters ----
```

```
Received:                0          3          0          0
VLAN Filtered:           0          0          0          0
Security Filtered:       0          0          0          0
Other Discards:          0          1          0          0
----  Egress Counters ----
Unicast:                 0          0          0          0
Multicast:               0          0          0          0
Broadcast:               0          0          0          0
Egress Filtered:         0          0          0          0
TailDrop:                0          0          0          0
Forward Restrict:        0          0          0          0
Congestion Filtered:     0          2          0          0
Control Packets:         4          0          0          0
----  Drop Counters ----
Drop Mode:               0          0          0          0
Drop Counter:            0          1          0          0

MUX PFE:                    4          5
------------------------------------------------------------------------
Drop Mode:                  0          0
Drop Count:                 0          0
```

show pfe data

Syntax

```
show pfe data
<"usp flow config">
<"usp flow stats">
```

Release Information

Command introduced in Junos OS Release 18.2R3-S3.

Starting in Junos OS Release 18.2R3-S3, 19.1R3, 19.2R3, 19.3R3, 19.4R2, 20.1R2, you can now view the Packet Forwarding Engine data using the **usp flow config** and **usp flow stats** options for the **show pfe data** command.

Description

Displays the Packet Forwarding Engine data. The Packet Forwarding Engine is the central processing element of the forwarding plane, systematically moving the packets in and out of the device. In Junos OS, the Packet Forwarding Engine has a locally stored forwarding table.

The forwarding table is a synchronized copy of all the information from the Route Engine that the forwarding plane needs to handle each packet, including outgoing interfaces, addresses, and so on. Storing a local copy of this information allows the Packet Forwarding Engine to get its job done without going to the control plane every time that it needs to process a packet.

The locally stored forwarding table allows the Packet Forwarding Engine to continue forwarding packets, even when a disruption occurs to the control plane, such as when a routing or other process issue happens.

Options

"usp flow config"—Displays current flow configuration in logical system root-logical-system.

"usp flow stats"—Displays current flow statistics.

Required Privilege Level

view

RELATED DOCUMENTATION

Junos OS Architecture Overview

List of Sample Output

show pfe data "usp flow config" on page 2574
show pfe data "usp flow stats" on page 2576

Output Fields

Table 213 on page 2569 lists the output fields for the **show pfe data** command. Output fields are listed in the approximate order in which they appear.

Table 213: show pfe data Output Fields

Field Name	Field Description
Flow main Parameters	

Table 213: show pfe data Output Fields *(continued)*

Field Name	Field Description
	Information about flow main parameters: • **allow-dns-reply**—Displays whether **allow-dns-reply** is enabled or disabled. • **allow-embedded-icmp**—Displays whether **allow-embedded-icmp** is enabled or disabled. • **mcast-buffer-enhance**—Displays whether **mcast-buffer-enhance** is enabled or disabled. • **allow-reverse-ecmp**—Displays whether **allow-reverse-ecmp** is enabled or disabled. • **no-local-favor-ecmp**—Displays whether **no-local-favor-ecmp** is enabled or disabled. • **Reordering-mixed-traffic**—Displays whether **Reordering-mixed-traffic** is enabled or disabled. • **Route-change-timeout**—Displays the route change timeout value. • **NH-resolve-timeout**—Displays next-hop resolve timeout value. • **Mcast-nh-resolve-retry**—Displays multicast next-hop resolve value. • **Pending-sess-queue-length**—Displays the pending session queue length. • **Syn-flood-protection tcp-syn-cookie**—Displays the synchronizing flood protection TCP synchronizing cookies. • **Syn-flood-dynamic-whitelist-time**—Displays the syncronizing floow dynamic allowlist time. • **no-inter-node-forwarding**—Displays whether **no-inter-node-forwarding** is enabled or disabled. • **no-inter-node-forwarding-ipv6**—Displays whether **no-inter-node-forwarding-ipv6** is enabled or disabled. • **enable-reroute-nat-check**—Displays whether **enable-reroute-nat-check** is enabled or disabled. • **force_ip_reassembly**—Displays whether **force_ip_reassembly** is enabled or disabled. • **fragment_limit**—Displays the fragment limit. • **frag_reassembly_timeout**—Displays the fragment reassembly timeout value. • **sync_icmp_session**—Displays whether **sync_icmp_session** is enabled or disabled. • **log dropped-icmp-packet**—Displays whether log **dropped-icmp-packet** is enabled or disabled. • **log dropped-illegal-packet**—Displays whether log **dropped-illegal-packet** is enabled or disabled. • **preserve incoming frag size**—Displays whether preserve incoming fragment size is enabled or disabled. • **log-extension**—Displays whether **log-extension** is enabled or disabled. • **advanced options drop_match_reserved_ip_address**—Displays whether advanced options **drop_match_reserved_ip_address** is enabled or disabled. • **advanced options drop_link_local_address**—Displays whether advanced options **drop_link_local_address** is enabled or disabled. • **advanced options reverse route packet mode vr option**—Displays whether advanced options reverse route packet mode vr option is enabled or disabled. • **advanced options close icmp session immediately**—Displays whether advanced options close Internet Control Message Protocol session immediately is enabled or disabled. • **load-distribution session-affinity ipsec**—Displays whether **load-distribution session-affinity**

Table 213: show pfe data Output Fields *(continued)*

Field Name	Field Description
	ipsec is enabled or disabled.
Aging Parameters	Information about aging parameters: • **early-ageout**—Displays the number of early ageout. • **low-watermark**—Displays the low watermark value. • **high-watermark**—Displays the high watermark value.
TCP MSS Parameters	Information about TCP MSS Parameters: • **all-tcp-mss**—Displays whether **all-tcp-mss** is enabled or disabled. • **ipsec-vpn-tcp-mss**—Displays whether **ipsec-vpn-tcp-mss** is enabled or disabled. • **gre-in-tcp-mss**—Displays whether **gre-in-tcp-mss** is enabled or disabled. • **gre-out-tcp-mss**—Displays whether **gre-out-tcp-mss** is enabled or disabled.
TCP Session Parameters	Information about TCP Session Parameters: • **rst-invalid-session**—Displays whether **rst-invalid-session** is enabled or disabled. • **fin-invalid-session**—Displays whether **fin-invalid-session** is enabled or disabled. • **rst-check-sequence**—Displays whether **rst-check-sequence** is enabled or disabled. • **syn-check**—Displays whether **syn-check** is enabled or disabled. • **syn-check-in-tunnel**—Displays whether **syn-check-in-tunnel** is enabled or disabled. • **sequence-check**—Displays whether **sequence-check** is enabled or disabled. • **strict-syn-check**—Displays whether **strict-syn-check** is enabled or disabled. • **tcp-initial-timeout**—Displays TCP initial timeout value. • **maximum-scale-window**—Displays the value of maximum scale window. • **time-wait-state-session-timeout**—Displays the wait time state and session timeout value.
Flow traceoptions	Information about flow traceoptions: • **trace flags**—Trace the flag option. • **trace level**—Trace level of the trace message. • **trace present**—Trace the present option. • **trace dst id**—Trace the specified destination ID. • **trace module buffer**—Trace the module buffer value.

Table 213: show pfe data Output Fields *(continued)*

Field Name	Field Description
Flow Modes	Information about flow modes: • **Flow mode for inet**—Flow mode packets to an IPv4 destination. Displays configuration and running mode. • **Flow mode for inet6**—Displays the IPv6 flow mode informations such as the running mode, configuration mode, and the status of IPv6 security knob. • **Flow mode for mpls**—Flow mode packets to MPLS. Displays configuration and running mode. • **Flow mode for iso**—Flow mode to ISO. Displays configuration and running mode.
Flow action flag	Information about the flow action flag.
Session distribution	• **Config mode**—Displays configuration mode. • **Running mode**—Displays running mode. • **GTP-U distribution**—Displays whether the GTP-U distribution is enabled or disabled.
Ipsec performance acceleration	Accelerate the IPSec traffic performance. Displays whether IPSec performance acceleration is enabled or disabled.
Packet ordering	Information about packet ordering: • **Config mode**—Displays configuration mode. • **Running mode**—Displays running mode.
Hash Bucket Size	Information about hash bucket size: • **Ipv4**—Display Packet Forwarding Engine IPv4 routes. • **Ipv6**—Display Packet Forwarding Engine IPv6 routes. • **Flow packet log enable**—Displays flow packet log enable. • **Flow packet log index**—Displays flow packet log index. • **Flow packet log throttle-interval**—Displays flow packet log throttle-interval. • **Flow tap mode**—Displays whether flow tap mode is enabled or disabled. • **Flow power mode IPsec**—Displays whether flow power mode IPsec is enabled or disabled. • **Fat core group global switch**—Displays whether fat core group global switch is on or off. • **Fat core group size**—Displays the fat core group size.

Table 213: show pfe data Output Fields *(continued)*

Field Name	Field Description
Ager Ring Statistics	Information about the ager ring statistics: • **IPv4 and IPv6 Common Ager Ring**—Displays whether batching is enabled or disabled. • **current tick**—Displays the current session timeout value. • **insert**—Displays the insert value. • **update**—Displays the update value. • **callback invoked**—Displays the callback invoked value. • **remove**—Displays the remove value. • **update skipped**—Displays the skipped update value. • **max watchdog time**—Displays maximum watchdog time. • **timeout value larger**—Displays larger timeout value. • **ager update**—Displays update ager value.
Session Scan stats	Information about session scan statistics: • **Requests recvd**—Displays the number of requests received. • **Requests Processing Done**—Displays the number of processing requests completed. • **Request Done Time**—Displays the number of requests done time. • **Skip session scan**—Displays the number of skip session scan. • **Total sessions scanned**—Displays the total number of sessions scanned. • **Batched (active sess limit)**—Displays the number of active sessions limit. • **Pending Que added**—Displays the number of pending queue added. • **Pending Que add fail**—Displays the number of pending queue add failures. • **Response Done**—Displays the number of response completed. • **Response Failed**—Displays the number of responses failed. • **Response Done Time**—Displays the response time completed. • **Scan Handler Invoked**—Displays the number of scan handler invoked. • **PendQ Handler Invoked**—Displays the number of pending handler invoked. • **Session scan running time**—Displays the timer of session scan running. • **Session scan handler yield**—Displays the number of session scan handler yield. • **Scan post even failed**—Displays the number of scan post even failed.

Table 213: show pfe data Output Fields *(continued)*

Field Name	Field Description
Flow Session Statistics	Information about flow session statistics: • **Current flows**—Displays the number of current flows. • **IPv4 flow alloc**—Displays the number of IPv4 flow allocation. • **IPv4 flow free**—Displays the number of IPv4 flow free. • **IPv4 flow alloc failure**—Displays the number of IPv4 flow allocation failures. • **IPv4 flow route skip**—Displays the number of IPv4 flow route skipped. • **IPv4 flow fast reroute**—Displays the number of IPv4 flow fast reroute. • **IPv4 flow tunnel route skip**—Displays the number of IPv4 flow tunnel route skipped. • **ager phase1**—Displays the number of ager phase1. • **ager phase2**—Displays the number of ager phase2. • **cp sess del rexmitted**—Displays the cp session delete rexmitted.
Flow Table Statistics	Information about the flow table statistics: • **flow add**—Displays number of flow add entries. • **flow remove**—Displays number of flow delete entries. • **flow find**—Displays number of flow find entries.

Sample Output

show pfe data "usp flow config"

`user@host>` **show pfe data "usp flow config"**

```
================ tnp_0x10000080 ================


Current FLOW configuration in logical system root-logical-system:
==========================

 Flow main Parameters::
  allow-dns-reply: disabled (default),
  allow-embedded-icmp: disabled (default),
  mcast-buffer-enhance: disabled (default),
  allow-reverse-ecmp: disabled (default),
  Reordering-mixed-traffic enabled (default),
  Route-change-timeout: 6 (default),
```

```
 Pending-sess-queue-length: 5 (default),
 Syn-flood-protection tcp-syn-cookie (default),
 Syn-flood-dynamic-whitelist-time 300,
 no-inter-node-forwarding: disabled (default),
 no-inter-node-forwarding-ipv6: disabled,
 enable-reroute-nat-check: disabled (default),
 force_ip_reassembly: disabled (default),
 sync_icmp_session: disabled (default),
 log dropped-icmp-packet: disabled (default),
 log dropped-illegal-packet: disabled (default),
  preserve incoming frag size : disabled
  log-extension : disabled (default)
 advanced options drop_match_reserved_ip_address: disabled (default),
 advanced options drop_link_local_address: disabled (default),
 advanced options reverse route packet mode vr option: disabled (default),
 advanced options close icmp session immediately: disabled (default),
 load-distribution session-affinity ipsec: disabled (default),
Aging Parameters::
 early-ageout: 20 (default),
 low-watermark: 100 (default),
 high-watermark: 100 (default),
TCP MSS Parameters::
 all-tcp-mss: disabled (default),
 ipsec-vpn-tcp-mss: disabled (default),
 gre-in-tcp-mss: disabled (default),
 gre-out-tcp-mss: disabled (default),
TCP Session Parameters::
 rst-invalid-session: disabled (default)
 fin-invalid-session: disabled (default)
 rst-check-sequence: disabled (default)
 syn-check: enabled (default)
 syn-check-in-tunnel: enabled (default)
 sequence-check: enabled (default)
 strict-syn-check: disabled (default)
 tcp-initial-timeout: 0x14 (default)
 maximum-scale-window: 0x3ebc0 (default)
 time-wait-state-session-timeout: 150 (default)
Flow traceoptions:
  trace flags: 0x0
  trace level: 0x0
  trace present: 0
  trace dst id: 0
  trace module buffer: 0
FLow Modes:
```

```
  Flow mode for inet:
   Running mode: FLOW_MODE_FLOW_BASED
   Config mode: FLOW_MODE_FLOW_BASED
  Flow mode for inet6:
   Running mode: FLOW_MODE_FLOW_BASED
   Config mode: FLOW_MODE_FLOW_BASED
   IPv6 security knob: enabled
  Flow mode for mpls:
   Running mode: FLOW_MODE_DROP
   Config mode: FLOW_MODE_DROP
  Flow mode for iso:
   Running mode: FLOW_MODE_DROP
   Config mode: FLOW_MODE_DROP
 Flow action flag: 0x700080
 Session distribution:
   Config mode: RR-based
   Running mode: RR-based
   GTP-U distribution: disabled
 Ipsec performance acceleration: disabled
 Packet ordering:
   Config mode: Hardware
   Running mode: Hardware
 Hash Bucket Size:
 Ipv4: 65536
 Ipv6: 65536
 Flow packet log enable: 0
 Flow packet log index: 20
 Flow packet log throttle-interval: 1024
 Flow tap mode: disabled(default)
```

Sample Output

show pfe data "usp flow stats"

`user@host>` **show pfe data "usp flow stats"**

```
================ tnp_0x10000080 ================

Ager Ring Statistics
        IPv4 and IPv6 Common Ager Ring: (Batching Disabled)
        current tick                        24929
        insert                              53082
```

```
        update                          10618908
        callback invoked                   53082
        remove                                 0
        update skipped                         0
        max watchdog time                   5000
        timeout value larger                   0
        ager update                            0


Session Scan stats
        Requests recvd                         0
        Requests Processing Done               0
        Request Done Time                      0
        Skip session scan                      0
        Total sessions scanned                 0
        Batched (active sess limit)            0
        Pending Que added                      0
        Pending Que add fail                   0
        Response Done                          0
        Response Failed                        0
        Response Done Time                     0
        Scan Handler Invoked                   0
        PendQ Handler Invoked                  0
        Session scan running time             40
        Session scan handler yield             0
        Scan post even failed                  0

Flow Session Statistics
        Current flows                          0
        IPv4 flow alloc                    26541
        IPv4 flow free                     26541
        IPv4 flow alloc failure                0
        IPv4 flow route skip                   0
        IPv4 flow fast reroute                 0
        IPv4 flow tunnel route skip            0
        ager phase1                        26541
        ager phase2                        26541
        cp sess del rexmitted                  0
Flow Table Statistics
        flow add                               0
        flow remove                            0
        flow find                      114370163
Ager Ring Statistics
        IPv4 and IPv6 Common Ager Ring: (Batching Disabled)
```

```
        current tick                        24929
        insert                              53082
        update                           10618908
        callback invoked                    53082
        remove                                  0
        update skipped                          0
        max watchdog time                    5000
        timeout value larger                    0
        ager update                             0



Flow Session Statistics
        Current flows                           0
        IPv6 flow alloc                         0
        IPv6 flow free                          0
        IPv6 flow alloc failure                 0
        IPv6 flow route skip                    0
        IPv6 flow fast reroute                  0
        IPv6 flow tunnel route skip             0
        ager phase1                             0
        ager phase2                             0
        cp sess del rexmitted                   0
Flow Table Statistics
        flow add                                0
        flow remove                             0
        flow find                               0
```

show system errors

Syntax

```
show system errors
<cb slot| ccg slot | fan slot | fpc slot | psm slot | re slot | sib slot>
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

Description

Display information about faults in the system. You can display all errors or the errors for one system component. Use this command to understand about faults and their correlation with other events. First, top level root causes are listed, with board level faults followed by component level faults. Next, details for affected faults are listed.

The show output represents five faults, F1 through F5. F4 and F5 are top level faults, where F4 is affected by F1, F2, and F3; and F3 is affected by F1 and F2. The lowest level (leaf) faults, F1, F2, and F5, have no affected events.

> **NOTE:** For Junos OS Evolved, only the QFX5200 supports this command. For all other Junos OS Evolved platforms, use the *show system errors active*, *show system errors count*, *show system errors error-id*, or *show system errors fru* command.

Options

This command has no options.

Required Privilege Level

view

RELATED DOCUMENTATION

show system errors history | 2583

List of Sample Output

show system errors on page 2580
show system errors fpc 0 on page 2581
show system errors sib 0 on page 2582

Output Fields

Table 214 on page 2580 lists the output fields for the **show system errors** command. Output fields are listed in the approximate order in which they appear.

Table 214: show system errors Output Fields

Field Name	Field Description
Top level root causes	Display of the top level faults with board level faults followed by component level faults.
Fx	Fault number F1 to Fn, where F1 is the first fault and n is the last fault generated by the system.
(*module*, *error-id*, *board-name*, *component-name*)	Information about the fault. Component level faults include the component name.
Group	Fault severity level is Fatal, Major, or Minor.
Scope	Affected scope of fault is System, Component, Board, or Link.
Corr-enabled	Correlation with fault is always enabled, Y.
Time	Time in the format yyyy-mm-dd hh:nn:ss.lll TMZ, where nn is minutes, lll is milliseconds, and TMZ is time zone.
Desc	Description of the fault.
Actions	List of errors that caused the fault.
Root-causes	List of faults that caused this error.
Affected	List of faults that correlate to this root cause.
Details for affected errors	Display the affected errors listed in top level faults.

Sample Output

show system errors

```
user@host> show system errors
```

```
Top level root-causes:
F4: {pciesw, 1, fpc0} Group: Fatal Scope: Board Corr-enabled: Y
Time: “2017-02-22 16:37:47.456 PST”
Desc: PCIe Switch Fatal AER Errors
Actions: Alarm: FPC_FATAL_ERRORS + FRU_FAULT
Root-causes: None
Affected:
F3: {hwd, 1, fpc0}
F1: {pechip, 1, fpc0, pechip0}
F2: {pechip, 1, fpc0, pechip3}
F5: {pfchip, 3, sib0, pfchip5} Group: Major Scope: Component Corr-enabled: Y
Time: “2017-02-22 18:37:47.456 PST”
Desc: Midplane link errors
Actions: Alarm: ASIC_FABRIC_LINK_ERRORS
Affected: None
Details for Affected Errors:
F3: {hwd, 1, fpc0}, Group: Fatal Scope: Board Corr-enabled: Y
Time: “2017-02-22 16:37:47.856 PST”
Desc: FPC Fault
Root-causes: F4 : { pciesw, 1, fpc0}
Affected:
F1: {pechip, 1, fpc0, pechip0}
F2: {pechip, 1, fpc0, pechip3}
F1: {pechip, 3, fpc0, pechip0}, Group: Fatal Scope: Component Corr-enabled: Y
Time: “2017-02-22 16:37:48.500 PST”
Desc: PIO Fault
Root-causes:
F4 : {pciesw, 1, fpc0}
Affected: None
F2: {pechip, 3, fpc0, pechip1}, Group: Fatal Scope: Component Corr-enabled: Y
Time: “2017-02-22 16:37:48.600 PST”
Desc: PIO Fault
Root-causes:
F4 : {pciesw, 1, fpc0}
Affected: None
```

show system errors fpc 0

user@host> **show system errors fpc 0**

```
Top level root-causes:
F4: {pciesw, 1, fpc0} Group: Fatal   Scope: Board  Corr-enabled: Y
  Time:    “2017-02-22 16:37:47.456 PST”
  Desc:    PCIe Switch Fatal AER Errors
```

```
    Actions: Alarm: FPC_FATAL_ERRORS + FRU_FAULT
    Root-causes: None
    Affected:
      F3:    {hwd, 1, fpc0}
      F1:    {pechip, 1, fpc0, pechip0}
      F2:    {pechip, 1, fpc0, pechip3}

Details for Affected Errors:
F3: {hwd, 1, fpc0}, Group: Fatal   Scope: Board  Corr-enabled: Y
    Time: “2017-02-22 16:37:47.856 PST”
  Desc:    FPC Fault
  Root-causes: F4 : { pciesw, 1, fpc0}
  Affected:
      F1:    {pechip, 1, fpc0, pechip0}
      F2:    {pechip, 1, fpc0, pechip3}

F1: {pechip, 3, fpc0, pechip0}, Group: Fatal   Scope: Component  Corr-enabled: Y
    Time: “2017-02-22 16:37:48.500 PST”
    Desc: PIO Fault
  Root-causes:
      F4 :   {pciesw, 1, fpc0}
  Affected: None
F2: {pechip, 3, fpc0, pechip1}, Group: Fatal   Scope: Component  Corr-enabled: Y
    Time: “2017-02-22 16:37:48.600 PST”
    Desc: PIO Fault
  Root-causes:
      F4 :   {pciesw, 1, fpc0}
  Affected: None
```

show system errors sib 0

user@host> **show system errors sib 0**

```
Top level root-causes:
F5: {pfchip, 3, sib0, pfchip5} Group: Major   Scope: Component  Corr-enabled: Y
  Time:    “2017-02-22 18:37:47.456 PST”
  Desc:    Midplane link errors
    Actions: Alarm: ASIC_FABRIC_LINK_ERRORS
    Affected: None
```

show system errors history

Syntax

```
show chassis errors history
<cb slot| ccg slot | fan slot | fpc slot | psm slot | re slot | sib slot>
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

Description

Display information about cleared faults in the error history buffer. You can display history for all errors or the errors for one system component. The error history is displayed in chronological order and includes a description of each PFE and FCHIP fault and when the fault was raised and cleared.

> **NOTE:** For Junos OS Evolved, only the QFX5200 supports this command. For all other Junos OS Evolved platforms, use the *show system errors active*, *show system errors count*, *show system errors error-id*, or *show system errors fru* command.

Options

This command has no options.

Required Privilege Level

view

RELATED DOCUMENTATION

show system errors | 2579

List of Sample Output

show system errors history on page 2584

Output Fields

Table 214 on page 2580 lists the output fields for the **show system errors history** command. Output fields are listed in the approximate order in which they appear.

Table 215: show system errors history Output Fields

Field Name	Field Description
Fault (*module*, *error-id*, *board-name/component-name*, *PFE-or-FCHIP*)	Information about the fault.
Group	Fault severity level is Fatal, Major, or Minor.
Scope	Affected scope of fault is System, Component, Board, or Link.
Corr-enabled	Correlation with fault is always enabled, Y.
Raised	Time the fault was raised, in the format yyyy-mm-dd hh:nn:ss.lll TMZ, where nn is minutes, lll is milliseconds, and TMZ is time zone.
Desc	Description of the fault.
Cleared	Time the fault was cleared, in the format yyyy-mm-dd hh:nn:ss.lll TMZ, where nn is minutes, lll is milliseconds, and TMZ is time zone.

Sample Output

show system errors history

`user@host>` **show system errors history**

```
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[0]}
 Group:   Major             Scope: Link          Corr-enabled: Y
 Raised:  2017-04-19 18:18:48.652000 PDT
 Desc:    Fabric Down condition on PFE
 Cleared: 2017-04-19 18:18:49.474975 PDT
 Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[1]}
 Group:   Major             Scope: Link          Corr-enabled: Y
 Raised:  2017-04-19 18:18:48.653000 PDT
 Desc:    Fabric Down condition on PFE
 Cleared: 2017-04-19 18:18:49.474668 PDT
 Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[2]}
 Group:   Major             Scope: Link          Corr-enabled: Y
 Raised:  2017-04-19 18:18:48.654000 PDT
```

```
 Desc:    Fabric Down condition on PFE
 Cleared: 2017-04-19 18:18:49.474245 PDT
 Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[3]}
 Group:   Major             Scope: Link           Corr-enabled: Y
 Raised:  2017-04-19 18:18:48.654000 PDT
 Desc:    Fabric Down condition on PFE
 Cleared: 2017-04-19 18:18:49.210875 PDT
 Fault: {pechip, 1143, /Chassis[0]/Fpc[4], Pfe[0]}
 Group:   Major             Scope: Component      Corr-enabled: N
 Raised:  2017-04-19 18:18:57.533000 PDT
 Desc:    hostif_local_int_wnack0
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[0]}
 Group:   Major             Scope: Link           Corr-enabled: Y
 Raised:  2017-04-19 19:45:20.949000 PDT
 Desc:    Fabric Down condition on PFE
 Cleared: Active
```

traceroute

List of Syntax

Syntax on page 2586
Syntax (QFX Series and OCX Series) on page 2586

Syntax

```
traceroute
<host>
<as-number-lookup>
<bypass-routing>
<ce-ip ip address>
<clns>
<ethernet host>
<gateway address>
<inet>
<inet6>
<interface interface-name>
<logical-system logical-system-name>
<monitor host>
<mpls (ldp FEC address | rsvp label-switched-path-name | bgp FEC address)>
<next-hop next-hop address>
<no-resolve host>
<overlay>
<port>
<propagate-ttl host>
<routing-instance routing-instance-name>
<tenant tenant-name>
<source source-address>
<tos value>
<ttl value>
<wait seconds>
```

Syntax (QFX Series and OCX Series)

```
traceroute
<host>
<as-number-lookup>
<bypass-routing>
<gateway address>
<inet>
<inet6>
<interface interface-name>
```

<monitor *host*>
<mpls (ldp *FEC address* | rsvp *label-switched-path-name* | bgp *FEC address*)>
<next-hop *next-hop address*>
<no-resolve *host*>
<overlay>
<port>
<propagate-ttl *host*>
<routing-instance *routing-instance-name*>
<source *source-address*>
<tos *value*>
<ttl *value*>
<wait *seconds*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
mpls option introduced in Junos OS Release 9.2.
propagate-ttl option introduced in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Support for IPv6 traceroute with **as-number-lookup** introduced with Junos OS Release 18.3R1.
The command **tenant** option is introduced in Junos OS Release 19.2R1 for the SRX Series.
The following options are deprecated in Junos OS Evolved Release 18.3R1: **logical-system** and **propagate-ttl**.

Description

Display the route that packets take to a specified network host. Use **traceroute** as a debugging tool to locate points of failure in a network.

Options

host—IP address or name of remote host.

as-number-lookup—(Optional) Display the autonomous system (AS) number of each intermediate hop on the path from the host to the destination.

bypass-routing—(Optional) Bypass the normal routing tables and send requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to display a route to a local system through an interface that has no route through it.

ce-ip *IPv4 or IPv6 address*—(MX Series routers with MPC and MIC interfaces only) (Optional) Check the route to a customer edge (CE) IP address in a virtual private LAN service (VPLS) and Ethernet VPN (EVPN) network.

clns—(Optional) Trace the route belonging to Connectionless Network Service (CLNS).

ethernet *host*—(Optional) Trace the route to an Ethernet host using unicast MAC address.

gateway *address*—(Optional) Address of a router or switch through which the route transits.

inet | inet6—(Optional) Trace the route belonging to IPv4 or IPv6, respectively.

interface *interface-name*—(Optional) Name of the interface over which to send packets.

logical-system (all | *logical-system-name*)—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Perform this operation on all logical systems or on a particular logical system.

tenant *tenant-name*—(Optional) Name of a particular tenant system for traceroute attempt.

monitor *host*—(Optional) Display real-time monitoring information for the specified host.

mpls (ldp *FEC address* | rsvp *label-switched-path name*)—(Optional) See **traceroute mpls ldp** and **traceroute mpls rsvp**.

next-hop—The next-hop through which to send packets to a destination.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

overlay—(Optional) Traceroute overlay path.

port—(Optional) Base port number to use in traceroute probes.

propagate-ttl—(Optional) On the PE routing device, use this option to view locally generated Routing Engine transit traffic. This is applicable for MPLS L3VPN traffic only.

Use for troubleshooting, when you want to view hop-by-hop information from the local provider router to the remote provider router, when TTL decrementing is disabled on the core network using the **no-proagate-ttl** configuration statement.

NOTE: Using **propagate-ttl** with **traceroute** on the CE router does not show hop-by-hop information.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the traceroute attempt.

source *source-address*—(Optional) Source address of the outgoing traceroute packets.

tos *value*—(Optional) Value to include in the IP type-of-service (ToS) field. The range of values is **0** through **255**.

ttl *value*—(Optional) Maximum time-to-live value to include in the traceroute request. The range of values is **0** through **128**.

wait *seconds*—(Optional) Maximum time to wait for a response to the traceroute request.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
network

RELATED DOCUMENTATION

traceroute monitor

List of Sample Output

traceroute on page 2590
traceroute as-number-lookup host on page 2590
traceroute no-resolve on page 2590
traceroute propogate-ttl on page 2591
traceroute (Between CE Routers, Layer 3 VPN) on page 2591
traceroute (Through an MPLS LSP) on page 2591
traceroute routing-instance no-resolve (Through an MPLS LSP) on page 2591
traceroute (Junos OS Evolved, Through an MPLS LSP) on page 2592

Output Fields

Table 216 on page 2589 describes the output fields for the **traceroute** command. Output fields are listed in the approximate order in which they appear.

Table 216: traceroute Output Fields

Field Name	Field Description
traceroute to	IP address of the receiver.
hops max	Maximum number of hops allowed.
byte packets	Size of packets being sent.
number-of-hops	Number of hops from the source to the named router or switch.
router-name	Name of the router or switch for this hop.
address	Address of the router or switch for this hop.
Round trip time	Average round-trip time, in milliseconds (ms).

Sample Output

traceroute

```
user@host> traceroute santacruz
```

```
traceroute to host1.example.com (10.156.169.254), 30 hops max, 40 byte packets
 1  blue23 (10.168.1.254)    2.370 ms  2.853 ms  0.367 ms
 2  red14  (10.168.255.250)  0.778 ms  2.937 ms  0.446 ms
 3  yellow (10.156.169.254)  7.737 ms  89.905 ms  0.834 ms
```

traceroute as-number-lookup host

```
user@host> traceroute as-number-lookup 10.100.1.1
```

```
traceroute to 10.100.1.1 (10.100.1.1), 30 hops max, 40 byte packets
 1  10.39.1.1 (10.39.1.1)  0.779 ms  0.728 ms  0.562 ms
 2  10.39.1.6 (10.39.1.6) [AS  32]  0.657 ms  0.611 ms  0.617 ms
 3  10.100.1.1 (10.100.1.1) [AS  10, 40, 50]  0.880 ms  0.808 ms  0.774 ms
```

```
user@host> traceroute as-number-lookup 1::1
```

```
traceroute6 to 1::1 (1::1) from 2001:b8::7, 64 hops max, 12 byte packets
```

```
user@host> traceroute 2001:b8::7 as-number-lookup
```

```
traceroute6 to 2001:b8::7 (2001:b8::7) from 2001:db8::9, 64 hops max, 12 byte
packets
 1  2001:db8::10 (2001:db8::10) [AS 18] 0.657 ms  17.319 ms  0.504 ms
 2  2001:b8::7 (2001:b8::7)  0.949 ms  0.930 ms  0.739 ms
```

traceroute no-resolve

```
user@host> traceroute santacruz no-resolve
```

```
traceroute to host1.example.com (10.156.169.254), 30 hops max, 40 byte packets
 1  10.168.1.254  0.458 ms  0.370 ms  0.365 ms
 2  10.168.255.250  0.474 ms  0.450 ms  0.444 ms
 3  10.156.169.254  0.931 ms  0.876 ms  0.862 ms
```

traceroute propogate-ttl

user@host> **traceroute propagate-ttl 100.200.2.2 routing-instance VPN-A**

```
traceroute to 100.200.2.2 (100.200.2.2) from 1.1.0.2, 30 hops max, 40 byte packets

 1  1.2.0.2 (1.2.0.2)  2.456 ms  1.753 ms  1.672 ms
     MPLS Label=299776 CoS=0 TTL=1 S=0
     MPLS Label=299792 CoS=0 TTL=1 S=1
 2  1.3.0.2 (1.3.0.2)  1.213 ms  1.225 ms  1.166 ms
     MPLS Label=299792 CoS=0 TTL=1 S=1
 3  100.200.2.2 (100.200.2.2)  1.422 ms  1.521 ms  1.443 ms
```

traceroute (Between CE Routers, Layer 3 VPN)

user@host> **traceroute vpn09**

```
traceroute to host2.example.com (10.255.14.179), 30 hops max, 40
      byte packets
       1  10.39.10.21 (10.39.10.21)  0.598 ms  0.500 ms  0.461 ms
       2  10.39.1.13 (10.39.1.13)  0.796 ms  0.775 ms  0.806 ms
           MPLS Label=100006 CoS=0 TTL=1 S=1
       3  host2.example.com (10.255.14.179)  0.783 ms  0.716 ms  0.686
```

traceroute (Through an MPLS LSP)

user@host> **traceroute mpls1**

```
traceroute to 10.168.1.224 (10.168.1.224), 30 hops max, 40 byte packets
 1  mpls1-sr0.company.net (10.168.200.101)  0.555 ms  0.393 ms  0.367 ms
     MPLS Label=1024 CoS=0 TTL=1
 2  mpls5-lo0.company.net (10.168.1.224)  0.420 ms  0.394 ms  0.401 ms
```

traceroute routing-instance no-resolve (Through an MPLS LSP)

user@host> **traceroute routing-instance VRF-1 198.51.100.1 no-resolve**

```
traceroute to 198.51.100.1 (198.51.100.1), 30 hops max, 40 byte packets
 1  198.51.100.20  20.243 ms  13.256 ms  24.194 ms
     MPLS Label=299792 CoS=0 TTL=1 S=0
```

```
     MPLS Label=16 CoS=0 TTL=1 S=1
 2  198.51.100.21  14.126 ms  13.090 ms  29.082 ms
     MPLS Label=16 CoS=0 TTL=1 S=0
     MPLS Label=16 CoS=0 TTL=2 S=1
 3  198.51.100.22  16.419 ms  11.564 ms  17.068 ms
     MPLS Label=16 CoS=0 TTL=1 S=1
 4  198.51.100.1  12.794 ms  12.939 ms  17.123 ms
```

traceroute (Junos OS Evolved, Through an MPLS LSP)

The Junos OS Evolved **traceroute** command parses MPLS data in the same way as the Linux **traceroute** command: L=label, E=exp_use, S=stack_bottom, and T=TTL. In the example below, **T=1/L=16** indicates the TTL with label 16.

`user@host>` **traceroute 192.0.2.50 ttl 255**

```
traceroute to 192.0.2.50 (192.0.2.50), 255 hops max, 60 byte packets
 1  192.0.2.60 (192.0.2.60)  13.565 ms  11.696 ms  11.448 ms
 2  192.0.2.61 (192.0.2.61) <MPLS:L=17,E=0,S=0,T=1/L=16,E=0,S=1,T=1>  34.034 ms
31.538 ms  27.697 ms
 3  192.0.2.62 (192.0.2.62) <MPLS:L=299776,E=0,S=0,T=1/L=16,E=0,S=1,T=2>  23.174
ms  24.393 ms  21.009 ms
 4  192.0.2.63 (192.0.2.63)  24.553 ms  19.698 ms  25.648 ms
 5  192.0.2.50 (192.0.2.50)  33.322 ms  29.514 ms  24.706 ms
```

CHAPTER 79

Operational Commands: Realtime Performance Monitoring

IN THIS CHAPTER

- show services rpm active-servers | 2594
- show services rpm history-results | 2596
- show services rpm probe-results | 2601

show services rpm active-servers

Syntax

```
show services rpm active-servers
```

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 13.2 for PTX Series Packet Transport routers.
Command introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Display the protocols and corresponding ports for which a router or switch is configured as a real-time performance monitoring (RPM) server.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show services rpm active-servers on page 2595

Output Fields

Table 217 on page 2594 lists the output fields for the **show services rpm active-servers** command. Output fields are listed in the approximate order in which they appear.

Table 217: show services rpm active-servers Output Fields

Field Name	Field Description
Protocol	Protocol configured on the receiving probe server. The protocol can be the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).
Port	Port configured on the receiving probe server.
Destination interface name	Output interface name for the probes.

Sample Output

show services rpm active-servers

user@host> **show services rpm active-servers**

```
    Protocol: TCP, Port: 50000, Destination interface name: lt-0/0/0.0
    Protocol: UDP, Port: 50001, Destination interface name: lt-0/0/0.0
```

show services rpm history-results

Syntax

```
show services rpm history-results
<brief | detail>
<dst-interface interface-name>
<owner owner>
<limit number>
<since time>
<source-address address>
<target-address address>
<test name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 on EX Series switches.
Command introduced in Junos OS Release 13.2 on PTX Series Packet Transport routers.
dst-interface, **limit**, **source-address**, and **target-address** options introduced in Junos OS Release 18.1R1 on MX Series.
owner and **test** options became optional in Junos OS Release 18.1R1 on MX Series.
Command introduced in Junos OS Release 18.1 on QFX Series switches.

Description

Display the results stored for the specified real-time performance monitoring (RPM) probes.

Options

none—(Optional) Display the results of the last 50 probes for all RPM instances.

brief | detail—(Optional) Display the specified level of output.

dst-interface *interface-name*—(Optional) Display information only for RPM probes that are generated on this MS-MPC or MS-MIC services interface. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

limit *number*—(Optional) Limit the number of results that are displayed. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

Range: 1 through 4,294,967,295

Default: 100

owner *owner*—(Optional) Display information only for probes with the specified probe owner. You must configure **owner** if you configure any of the following options: **dst-interface**, **limit**, **source-address**, or **target-address**.

since *time*—(Optional) Display information from the specified time. Specify time as ***yyyy-mm-dd.hh:mm:ss***.

source-address *address*—(Optional) Display information only for probes with the specified source address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

target-address *address*—(Optional) Display information only for probes with the specified target address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

test *name*—(Optional starting in Junos OS Release 18.1R1) Display information only for the specified test.

Do not configure **test** if you configure any of the following options: **dst-interface**, **limit**, **source-address**, or **target-address**. These options do not work when you configure **test**.

Required Privilege Level
view

List of Sample Output
show services rpm history-results owner test on page 2598
show services rpm history-results owner test detail on page 2599

Output Fields
Table 218 on page 2597 lists the output fields for the **show services rpm history-results** command. Output fields are listed in the approximate order in which they appear.

Table 218: show services rpm history-results Output Fields

Field Name	Field Description	Level of Output
Owner	Probe owner.	All levels
Test	Name of a test for a probe instance.	All levels
Probe received	Timestamp when the probe result was determined.	All levels
Round trip time	Average ping round-trip time (RTT), in microseconds.	All levels
Probe results	Result of a particular probe performed by a remote host. The following information is contained in the results: • **Response received**—Timestamp when the probe result was determined. • **Rtt**—Average ping round-trip time (RTT), in microseconds.	**detail**

Table 218: show services rpm history-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over current test	Displays the results for the current test by probe at the time each probe was completed, as well as the status of the current test at the time the probe was completed.	**detail**
Probes sent	Number of probes sent with the current test.	**detail**
Probes received	Number of probe responses received within the current test.	**detail**
Loss percentage	Percentage of lost probes for the current test.	**detail**
Measurement	Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-pin-timestamp, the egress and ingress delay: • **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. • **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. • **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. • **Jitter**—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test. • **Stddev**—Standard deviation of the round-trip time, in microseconds, measured over the course of the current test.	**detail**

Sample Output

show services rpm history-results owner test

```
user@host> show services rpm history-results owner p1 test t1

     Owner, Test                 Probe received              Round trip time
    p1, t1                     Wed Aug 12 01:02:35 2009             315 usec
    p1, t1                     Wed Aug 12 01:02:36 2009             266 usec
    p1, t1                     Wed Aug 12 01:02:37 2009             314 usec
    p1, t1                     Wed Aug 12 01:02:38 2009             388 usec
```

```
p1, t1                      Wed Aug 12 01:02:39 2009             316 usec
p1, t1                      Wed Aug 12 01:02:40 2009             271 usec
p1, t1                      Wed Aug 12 01:02:41 2009             314 usec
p1, t1                      Wed Aug 12 01:02:42 2009            1180 usec
```

show services rpm history-results owner test detail

user@host> **show services rpm history-results owner p1 test t1 detail**

```
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:35 2009,
  Client and server hardware timestamps
  Rtt: 315 usec
Results over current test:
  Probes sent: 1, Probes received: 1, Loss percentage: 0
  Measurement: Round trip time
    Samples: 1, Minimum: 315 usec, Maximum: 315 usec, Average: 315 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 315 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:36 2009,
  Client and server hardware timestamps
  Rtt: 266 usec, Round trip jitter: -50 usec,
  Round trip interarrival jitter: 3 usec
Results over current test:
  Probes sent: 2, Probes received: 2, Loss percentage: 0
  Measurement: Round trip time
    Samples: 2, Minimum: 266 usec, Maximum: 315 usec, Average: 291 usec,
    Peak to peak: 49 usec, Stddev: 24 usec, Sum: 581 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:37 2009,
  Client and server hardware timestamps
  Rtt: 314 usec, Round trip jitter: 49 usec,
  Round trip interarrival jitter: 6 usec
Results over current test:
  Probes sent: 3, Probes received: 3, Loss percentage: 0
```

```
  Measurement: Round trip time
    Samples: 3, Minimum: 266 usec, Maximum: 315 usec, Average: 298 usec,
    Peak to peak: 49 usec, Stddev: 23 usec, Sum: 895 usec
  Measurement: Positive round trip jitter
    Samples: 1, Minimum: 49 usec, Maximum: 49 usec, Average: 49 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 49 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:38 2009,
  Client and server hardware timestamps
  Rtt: 388 usec, Round trip jitter: 74 usec,
  Round trip interarrival jitter: 10 usec
Results over current test:
  Probes sent: 4, Probes received: 4, Loss percentage: 0
  Measurement: Round trip time
    Samples: 4, Minimum: 266 usec, Maximum: 388 usec, Average: 321 usec,
    Peak to peak: 122 usec, Stddev: 44 usec, Sum: 1283 usec
  Measurement: Positive round trip jitter
    Samples: 2, Minimum: 49 usec, Maximum: 74 usec, Average: 62 usec,
    Peak to peak: 25 usec, Stddev: 12 usec, Sum: 123 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec
```

show services rpm probe-results

Syntax

```
show services rpm probe-results
<dst-interface interface-name>
<limit number>
<owner owner>
<source-address address>
<status (fail | pass) >
<target-address address>
<terse>
<test name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 on EX Series switches.
Command introduced in Junos OS Release 13.2 on PTX Series Packet Transport Series routers.
dst-interface, **limit**, **source-address**, **status**, **target-address**, and **terse** options introduced in Junos OS Release 18.1R1 on MX Series.
Command introduced in Junos OS Release 18.1 on QFX Series switches.

Description

Display the results of the most recent real-time performance monitoring (RPM) probes.

Options

All the following options require that you also configure the **owner** option.

dst-interface *interface-name*—(Optional) Display information only for RPM probes that are configured on this MS-MPC or MS-MIC services interface. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

limit *number*—(Optional) Limit the number of results that are displayed. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

Range: 1 through 4,294,967,295

Default: 100

none—Display information for all of the most recent RPM probes.

owner *owner*—(Optional) Display information only for probes with the specified probe owner. You must configure **owner** if you configure any other options.

source-address *address*—(Optional) Display information only for probes with the specified source address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

status—(Optional) Display information only for probes with the specified type of test result. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. Specify one of the following:

fail—Failed tests

pass—Passed tests

target-address *address*—(Optional) Display information only for probes with the specified target address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

terse—(Optional) Display summary information. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

test *name*—(Optional) Display information only for the specified test.

Do not configure **test** if you configure any of the following options: **dst-interface**, **source-address**, or **target-address**. These options do not work when you configure **test**.

Required Privilege Level
view

List of Sample Output
show services rpm probe-results (IPv4 Targets) on page 2609
show services rpm probe-results (IPv6 Targets) on page 2612
show services rpm probe-results owner terse on page 2613
show services rpm probe-results owner status fail on page 2613
show services rpm probe-results (BGP Neighbor Discovery) on page 2613

Output Fields
Table 219 on page 2602 lists the output fields for the **show services rpm probe-results** command. Output fields are listed in the approximate order in which they appear.

Table 219: show services rpm probe-results Output Fields

Field Name	Field Description	Level of Output
Owner	Owner name. When you configure the probe owner statement at the **[edit services rpm]** hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-Bgp-Owner.**	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Test	Name of a test representing a collection of probes. When you configure the test test-name statement at the **[edit services rpm probe owner]** hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-BGP-Test-** *n*, where *n* is a cumulative number.	All levels
Target address	Destination IPv4 address used for the probes. This field is displayed when the probes are sent to the configured IPv4 or IPv6 targets or RPM servers.	none **dst-interface limit owner source-address target-address terse test**
Target inet6-address	Destination IPv6 address used for the probes. This field is displayed when the probes are sent to the configured IPv6 targets or RPM servers.	none **dst-interface limit owner source-address target-address terse test**
Source address	Source address used for the probes.	none **dst-interface limit owner source-address target-address test**
Probe type	Protocol configured on the receiving probe server: **http-get, http-metadata-get, icmp-ping, icmp-ping-timestamp, tcp-ping, udp-ping,** or **udp-ping-timestamp**.	none **dst-interface limit owner source-address target-address test**
Test size	Number of probes within a test.	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Routing Instance Name	(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured: • When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash **(/)** is used to separate the two entities. For example, if the routing instance called **R1** is configured within the logical system called **LS**, the name in the output field is **LS/R1**. • When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance. • When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by **default**. A slash (/) is used to separate the two entities. For example, **LS/default**.	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output

Probe results	Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:
	• **Response received**
	  ◦ **Probe sent time**—Timestamp when the probe's results was sent.
	  ◦ **Probe rcvd/timeout time**—Timestamp when the probe's results was received.
	• **Client and server hardware timestamps**—If timestamps are configured, an entry appears at this point.
	• **Rtt**—Average ping round-trip time (RTT), in microseconds.
	• **Egress jitter**—Egress jitter, in microseconds.
	• **Ingress jitter**—Ingress jitter, in microseconds.
	• **Round trip jitter**—Round-trip jitter, in microseconds.
	• **Egress interarrival jitter**—Egress interarrival jitter, in microseconds.
	• **Ingress interarrival jitter**—Ingress interarrival jitter, in microseconds.
	• **Round trip interarrival jitter**—Round-trip interarrival jitter, in microseconds.
		none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over current test	Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes. • **Probes sent**—Number of probes sent within the current test. • **Probes received**—Number of probe responses received within the current test. • **Loss percentage**—Percentage of lost probes for the current test. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over last test	Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed • **Probes sent**—Number of probes sent for the most recently completed test. • **Probes received**—Number of probe responses received for the most recently completed test. • **Loss percentage**—Percentage of lost probes for the most recently completed test. • **Test completed**—Time the most recent test was completed. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over all tests	Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test. • **Probes sent**—Number of probes sent in all tests. • **Probes received**—Number of probe responses received in all tests. • **Loss percentage**—Percentage of lost probes in all tests. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types **icmp-ping-timestamp** and **udp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 219: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Error Stats	Displays error statistics for each probe. • **Invalid client recv timestamp**—Number of client receive timestamp less than client send timestamp. • **Invalid server send timestamp**—Number of server send timestamp less than server receive timestamp. • **Invalid server processing time**—Number of server side spent time greater than RTT. NOTE: **Error Stats** is displayed in the output only if non-zero statistics exists.	none **dst-interface limit owner source-address target-address test**
Last Probe Status	Status of the last probe that was sent for the current test (**fail** or **pass**).	**status**
Status	Status of the last completed test (**up** or **down**).	**status terse**
Source-IF	The MS-MPC or MS-MIC services interface that generates the RPM probes.	**terse**

Sample Output

show services rpm probe-results (IPv4 Targets)

`user@host>` **show services rpm probe-results**

```
Owner: ADSN-J4300.ADSN-J2300.D2, Test: 75300002
Target address: 172.16.54.172, Source address: 10.206.0.1,
Probe type: udp-ping-timestamp, Test size: 10 probes
Probe results:
  Response received
  Probe sent time: Tue Feb  6 14:53:15 2007,
  Probe rcvd/timeout time: Tue Feb 6 14:53:15 2007
  Client and server hardware timestamps
  Rtt: 575 usec, Egress jitter: 5 usec, Ingress jitter: 8 usec,
  Round trip jitter: 12 usec, Egress interarrival jitter: 8 usec,
 Ingress interarrival jitter: 7 usec, Round trip interarrival jitter: 7 usec,

  Round trip interarrival jitter: 669 usec
```

```
Results over current test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec,  Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over last test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Test completed on Tue Feb  6 14:53:16 2007
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
```

```
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over all tests:
  Probes sent: 560, Probes received: 560, Loss percentage: 0
  Measurement: Round trip time
    Samples: 560, Minimum: 805 usec, Maximum: 3114 usec, Average: 1756 usec,
    Peak to peak: 2309 usec, Stddev: 519 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 257, Minimum: 0 usec, Maximum: 2054 usec, Average: 597 usec,
    Peak to peak: 2054 usec, Stddev: 427 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 302, Minimum: 1 usec, Maximum: 1812 usec, Average: 511 usec,
    Peak to peak: 1811 usec, Stddev: 408 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
```

```
   Error Stats:
       Invalid client recv timestamp: 3, Invalid server send timestamp: 0
       Invalid server processing time: 0
```

show services rpm probe-results (IPv6 Targets)

`user@host>` **show services rpm probe-results**

```
   Owner: p, Test: t1
   Target inet6-address: 2001:db8:0:1:2a0:a502:0:1da,
   Target Port : 34567 Test size: 1000000 probes
   Probe results:
     Response received
     Probe sent time: Mon Dec 16 10:48:07 2013
     Probe rcvd/timeout time: Mon Dec 16 10:48:07 2013
     Client and server hardware timestamps
     Rtt: 236 usec, Round trip jitter: -10 usec, Round trip interarrival jitter:
484 usec
   Results over current test:
     Probes sent: 10, Probes received: 10, Loss percentage: 0
     Measurement: Round trip time
      Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec, Peak
to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
     Measurement: Positive round trip jitter
       Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
     Measurement: Negative round trip jitter
       Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec
   Results over last test:
     Probes sent: 10, Probes received: 10, Loss percentage: 0
     Test completed on Mon Dec 16 10:48:07 2013
     Measurement: Round trip time
      Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec, Peak
to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
     Measurement: Positive round trip jitter
       Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
     Measurement: Negative round trip jitter
       Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec
   Results over all tests(From start of current control session):
     Probes sent: 490, Probes received: 488, Loss percentage: 0
     Measurement: Round trip time
```

```
        Samples: 488, Minimum: 231 usec, Maximum: 306 usec, Average: 270 usec,
Peak to peak: 75 usec, Stddev: 16 usec, Sum: 131586 usec
      Measurement: Positive round trip jitter
        Samples: 254, Minimum: 0 usec, Maximum: 10151 usec, Average: 157 usec,
Peak to peak: 10151 usec, Stddev: 873 usec, Sum: 39817 usec
      Measurement: Negative round trip jitter
        Samples: 233, Minimum: 1 usec, Maximum: 10170 usec, Average: 171 usec,
Peak to peak: 10169 usec, Stddev: 888 usec, Sum: 39889 usec
```

show services rpm probe-results owner terse

user@host> **show services rpm probe-results owner owner1 terse**

```
Test Name      Source-IF           Target Address      Status       Last Change
t_1            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S

t_2            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S

t_3            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S
```

show services rpm probe-results owner status fail

user@host> **show services rpm probe-results owner owner1 status fail**

```
Test Name              Last Probe Status         Status
t_1                    FAIL                      DOWN
t_2                    FAIL                      DOWN
t_3                    FAIL                      DOWN
```

show services rpm probe-results (BGP Neighbor Discovery)

user@host> **show services rpm probe-results**

```
Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
    Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
    Routing Instance Name: LS1/RI1
    Probe results:
      Response received
      Probe sent time: Fri Oct 28 05:20:23 2005
      Probe rcvd/timeout time: Fri Oct 28 05:20:23 2005
      Rtt: 662 usec
    Results over current test:
```

```
  Probes sent: 5, Probes received: 5, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
    Jitter: 133 usec, Stddev: 53 usec
Results over all tests:
  Probes sent: 5, Probes received: 5, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
    Jitter: 133 usec, Stddev: 53 usec
```

CHAPTER 80

Operational Commands: Analyzers and Port Mirroring

IN THIS CHAPTER

- show analyzer | **2616**

show analyzer

Syntax

```
show analyzer analyzer-name
```

Release Information

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

Description

Display information about analyzers configured for mirroring.

Options

analyzer-name—(Optional) Displays the status of a specific analyzer on the switch.

Required Privilege Level

view

List of Sample Output

show analyzer on page 2617

Output Fields

Table 220 on page 2616 lists the output fields for the **command-name** command. Output fields are listed in the approximate order in which they appear.

Table 220: show analyzer Output Fields

Field Name	Field Description
Analyzer name	Displays the name of the analyzer.
Output interface	Specifies a local interface to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Output VLAN	Specifies a VLAN to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Mirror ratio	Displays the ratio of packets to be mirrored.
Egress monitored interfaces	Displays interfaces for which traffic exiting the interfaces is mirrored.
Ingress monitored interfaces	Displays interfaces for which traffic entering the interfaces is mirrored.
Ingress monitored VLANs	Displays VLANs for which traffic entering the VLAN is mirrored.

Sample Output

show analyzer

user@host> **show analyzer**

```
Analyzer name           : employee-monitor
  Output interface             : ge-0/0/10.0
  Output VLAN                  : remote-analyzer
  Mirror ratio                 : 1
  Loss priority                : High
  Egress monitored interfaces  : ge-0/0/3.0
  Ingress monitored interfaces : ge-0/0/0.0
  Ingress monitored interfaces : ge-0/0/1.0
```

CHAPTER 81

Operational Commands: sFlow Monitoring Technology

IN THIS CHAPTER

- clear sflow collectors statistics | **2619**
- clear sflow collector statistics (QFX Series) | **2620**
- show sflow | **2622**
- show sflow collector | **2625**
- show sflow interface | **2628**

clear sflow collectors statistics

Syntax

```
clear sflow collectors statistics
```

Release Information

Command introduced in JUNOS Release 9.5 for EX Series switches.

Description

Clear the sFlow collector's statistics.

Required Privilege Level

clear

RELATED DOCUMENTATION

Configuring sFlow Technology for Network Monitoring (CLI Procedure) | 997

Sample Output

```
clear sflow collectors statistics
```

clear sflow collector statistics (QFX Series)

Syntax

```
clear sflow collector statistics
```

Release Information

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.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Clear the sample counters for all sFlow collectors.

Required Privilege Level

view

RELATED DOCUMENTATION

Example: Monitoring Network Traffic Using sFlow Technology | 999

show sflow collector | 2625

List of Sample Output

clear sflow collector statistics on page 2620

Sample Output

clear sflow collector statistics

The following example shows two output examples for the **show sflow collector** command, one before and one after the **clear sflow collector statistics** command was issued.

`user@host>` **show sflow collector**

```
Collector        Udp-port    No. of samples
   address
```

```
    10.1.1.1            6343        3174
    10.1.2.1            6343        3562
```

user@host> **clear sflow collector statistics**

user@host> **show sflow collector**

```
Collector        Udp-port    No. of samples
    address
    10.1.1.1            6343        0
    10.1.2.1            6343        0
```

show sflow

Syntax

```
show sflow
<collector>
<interface>
```

Release Information

Command introduced in Junos OS Release 9.3 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.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Display sFlow configuration information.

Options

none— Display all sFlow configuration information.

collector—(Optional) Display a list of configured sFlow collectors and their properties. See **show sflow collector**.

interface—(Optional) Display the interfaces on which sFlow technology is enabled and the sampling parameters. See **show sflow interface**.

Required Privilege Level

view

RELATED DOCUMENTATION

- show sflow interface | **2628**
- show sflow collector | **2625**
- clear sflow collector statistics (QFX Series) | **2620**
- Example: Monitoring Network Traffic Using sFlow Technology | **999**
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

List of Sample Output

show sflow on page 2623

Output Fields

Table 221 on page 2623 lists the output fields for the **show sflow** command. Output fields are listed in the approximate order in which they appear.

Table 221: show sflow Output Fields

Field Name	Field Description
sFlow	Status of the feature: **Enabled** or **Disabled**.
Adaptive fallback	Reverts back to the previously configured adaptive sample rate. Adaptive fallback is triggered when the number of samples per second for each FPC is less than the sample-limit threshold value. This option is disabled by default.
Sample limit	Number of packets sampled per second. This sample limit cannot be configured and is set to 300 packets per second.
Sample limit threshold	Threshold value that you explicitly configure for adaptive sampling fallback.
Polling interval	Interval at which the sFlow agent polls the interface.
Sample rate egress	Rate at which egress packets are sampled.
Sample rate ingress	Rate at which ingress packets are sampled.
Agent ID	IP address assigned to the sFlow agent.
Source IP address	Source IP address for the sFlow packets.
Agent ID IPv6	IPv6 address assigned to the sFlow agent.
Source IPv6 address	Source IPv6 address for the sFlow packets.

Sample Output

show sflow

```
user@host> show sflow
```

```
sFlow                   : Enabled
Adaptive fallback       : Disabled
Sample limit            : 300 packets/second
Sample limit threshold  : 150 packets/second
Polling interval        : 20 second
```

```
Sample rate egress      : 1:2048: Disabled
Sample rate ingress     : 1:1000: Enabled
Agent ID                : 10.93.54.7
Source IP address       : 10.93.54.7
```

show sflow collector

Syntax

```
show sflow collector
<brief | detail>
<address>
```

Release Information

Command introduced in Junos OS Release 9.3 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.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Display a list of configured sFlow collectors and their properties. Use the **address** option to display the information for a single collector address.

Required Privilege Level

view

RELATED DOCUMENTATION

- clear sflow collector statistics (QFX Series) | **2620**
- show sflow | **2622**
- show sflow interface | **2628**
- Example: Monitoring Network Traffic Using sFlow Technology | **999**
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches | **985**
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) | **997**

List of Sample Output

show sflow collector brief on page 2626
show sflow collector detail on page 2626

Output Fields

Table 222 on page 2626 lists the output fields for the **show sflow collector** command. Output fields are listed in the approximate order in which they appear.

Table 222: show sflow collector Output Fields

Field Name	Field Description	Level of Output
Collector address	IP address of the collector.	All levels
Udp-Port	UDP port number of the collector.	All levels
Dscp	Differentiated Services Code Point (DSCP) values applied to all packets for the collector.	All levels
Forwarding-Class	Forwarding-class values applied to all packets destined for the collector.	All levels
No. of samples	Number of samples collected.	All levels
Number of Counter Samples	Number of counter samples collected.	**detail**
Number of Flow Sample	Number of flow samples collected.	**detail**
Number of Datagrams	Number of datagrams collected.	**detail**

Sample Output

show sflow collector brief

```
user@host> show sflow collector brief
```

```
Collector            Udp-port    Dscp     Forwarding-Class     No. of samples
 address
10.213.0.191         6343        0        best-effort          23259
```

You get the same output for **show sflow collector address 10.213.0.191 brief**.

show sflow collector detail

```
user@host> show sflow collector detail
```

```
  Sflow Collector Information
    Collector Address: 10.213.0.191, Collector UDP Port: 6343
    DSCP Value: 0, Forwarding Class: best-effort
```

```
    Number of Counter Samples: 2724, Number of Flow Samples: 11
    Number of Samples: 23306, Number of Datagrams: 1509
```

You get the same output for **show sflow collector address 10.213.0.191 detail**.

show sflow interface

Syntax

```
show sflow interface
<interface-name interface-name>
```

Release Information

Command introduced in Junos OS Release 9.3 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.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.
interface-name *interface-name* option introduced.

Description

Display the interfaces on which sFlow is enabled and the sampling parameters for the interface. Use the **interface-name *interface-name*** option to get the sFlow interfaces information for a specific interface.

Required Privilege Level

view

RELATED DOCUMENTATION

- show sflow | 2622
- show sflow collector | 2625
- Example: Monitoring Network Traffic Using sFlow Technology | 999

List of Sample Output

show sflow interface interface-name on page 2629
show sflow interface (EX Series) on page 2629
show sflow interface (QFX Series Switch) on page 2629
show sflow interface (QFX3500 Switch in Standalone Mode) on page 2630
show sflow interface (QFX3500 Switch in Standalone Mode) on page 2630
show sflow interface (QFX3500 Switch in Standalone Mode) on page 2630
show sflow interface (QFX3500 Switch in Standalone Mode) on page 2631
show sflow interface (QFabric System) on page 2631

Output Fields

Table 223 on page 2629 lists the output fields for the **show sflow interface** command. Output fields are listed in the approximate order in which they appear.

Table 223: show sflow interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which sFlow technology is enabled.	All levels
Status Egress	Indicates whether an egress sample rate is enabled.	All levels
Status Ingress	Indicates whether an ingress sample rate is enabled.	All levels
Sample rate Egress	Rate at which egress packets are sampled.	All levels
Sample rate Ingress	Rate at which ingress packets are sampled.	All levels
Adapted sample rate Egress	Adapted rate at which egress packets are sampled.	All levels
Adapted sample rate Ingress	Adapted rate at which ingress packets are sampled.	All levels
Polling-interval	Interval at which the sFlow agent polls the interface.	All levels

Sample Output

show sflow interface interface-name

```
user@host> show sflow interface interface-name et-0/0/1
```

```
Interface       Status           Sample           Adapted          Polling
                                 rate             sample rate      interval

               Egress  Ingress   Egress Ingress  Egress Ingress
et-0/0/1.0     Enabled Enabled   100     100      800     800       20
```

show sflow interface (EX Series)

```
Interface       Status     Sample rate    Adapted sample rate   Polling-interval

            Egress Ingress   Egress Ingress   Egress Ingress
ge-0/0/0.0  Enabled  Disabled  1000    2048    1000     2048           20
```

show sflow interface (QFX Series Switch)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
ge-0/0/13.0   Enabled  Enabled  100    100   800    800           20
ge-1/0/15.0   Enabled  Enabled  100    100   400    400           20
ge-1/0/20.0   Enabled  Enabled  10     10    160    160           20
ge-1/0/21.0   Enabled  Enabled  10     10    10     10            20
```

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048           20
xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048           20
```

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048           20
xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048           20
```

Sample Output

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048           20
xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048           20
```

Sample Output

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048            20
xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048            20
```

Sample Output

show sflow interface (QFabric System)

```
user@host> show sflow interface
```

```
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
node1:xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048
20
node2:xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048
20
node4:xe-1/0/0.0    Enabled  Disabled  1000    2048    1000     2048
20
```

CHAPTER 82

Operational Commands: Ethernet OAM Connectivity Fault Management

IN THIS CHAPTER

- clear oam ethernet connectivity-fault-management delay-statistics | 2634
- clear oam ethernet connectivity-fault-management sla-iterator-statistics | 2636
- clear oam ethernet connectivity-fault-management statistics | 2638
- clear oam ethernet connectivity-fault-management continuity-measurement | 2640
- clear oam ethernet connectivity-fault-management linktrace path-database | 2642
- clear oam ethernet connectivity-fault-management loss-statistics | 2643
- clear oam ethernet connectivity-fault-management policer | 2645
- clear oam ethernet connectivity-fault-management statistics | 2647
- clear oam ethernet connectivity-fault-management synthetic-loss-measurement | 2649
- monitor ethernet delay-measurement | 2651
- monitor ethernet delay-measurement | 2657
- monitor ethernet loss-measurement | 2663
- monitor ethernet synthetic-loss-measurement | 2669
- monitor ethernet synthetic-loss-measurement | 2674
- show oam ethernet connectivity-fault-management delay-statistics | 2679
- show oam ethernet connectivity-fault-management forwarding-state | 2684
- show oam ethernet connectivity-fault-management forwarding-state | 2689
- show oam ethernet connectivity-fault-management interfaces | 2694
- show oam ethernet connectivity-fault-management path-database | 2702
- show oam ethernet connectivity-fault-management mep-database | 2705
- show oam ethernet connectivity-fault-management mip | 2712
- show oam ethernet connectivity-fault-management sla-iterator-statistics | 2714
- show oam ethernet connectivity-fault-management interfaces | 2727
- show oam ethernet connectivity-fault-management linktrace path-database | 2741
- show oam ethernet connectivity-fault-management loss-statistics | 2744
- show oam ethernet connectivity-fault-management mep-database | 2749
- show oam ethernet connectivity-fault-management mep-statistics | 2764

- show oam ethernet connectivity-fault-management path-database | **2780**
- show oam ethernet connectivity-fault-management policer | **2782**
- show oam ethernet connectivity-fault-management sla-iterator-statistics | **2786**
- show oam ethernet connectivity-fault-management synthetic-loss-statistics | **2799**
- show oam ethernet evc | **2802**
- show oam ethernet fnp interface | **2804**
- show oam ethernet fnp messages | **2806**
- show oam ethernet fnp status | **2808**
- show oam ethernet lmi | **2810**
- show oam ethernet lmi statistics | **2812**

clear oam ethernet connectivity-fault-management delay-statistics

Syntax

```
clear oam ethernet connectivity-fault-management delay-statistics
maintenance-association maintenance-association-name
maintenance-domain maintenance-domain-name
<logical-system logical-system-name>
<one-way>
<two-way>
```

Release Information

Command introduced in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.4 for EX Series switches.

Description

On MX Series routers and EX Series switches, clear ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM) delay statistics and ETH-DM frame counts.

Options

maintenance-association *maintenance-association-name*—Clear ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association.

maintenance-domain *maintenance-domain-name*—Clear ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance domain.

logical-system *logical-system-name*—(MX Series routers only) (Optional) Clear ETH-DM delay statistics and ETH-DM frame counts for the specified logical system.

one-way—(Optional) Clear one-way ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association, maintenance domain, or (on the routers only) logical system.

two-way—(Optional) Clear two-way ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association, maintenance domain, or (on the routers only) logical system.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2647
show oam ethernet connectivity-fault-management delay-statistics | 2679
show oam ethernet connectivity-fault-management interfaces | 2727

List of Sample Output

clear oam ethernet connectivity-fault-management delay statistics on page 2635

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management delay statistics

```
user@switch> clear oam ethernet connectivity-fault-management delay-statistics maintenance-domain
md1 maintenance-association ma1

Delay statistics entries cleared
```

clear oam ethernet connectivity-fault-management sla-iterator-statistics

Syntax

clear oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-association ***maintenance-association-name***
maintenance-domain *maintenance-domain-name*
<local-mep ***local-mep-id>***
<remote-mep *remote-mep-id>*
sla-iterator *sla-iterator*

Release Information
Command introduced in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 13.2 for MX Series routers.

Description
Clear Ethernet Operation, Administration, and Maintenance (OAM) service-level agreement (SLA) iterator statistics. For MX Series routers, clear the SLA iterator statistics and proactive Ethernet synthetic loss measurement (ETH-SLM) statistics.

Options
maintenance-association ***maintenance-association-name***—Name of the maintenance association.

maintenance-domain ***maintenance-domain-name***—Name of the maintenance domain.

local-mep ***local-mep-id***—(Optional) Identifier of the local MEP.

remote-mep ***remote-mep-id***—(Optional) Identifier of the remote MEP.

sla-iterator ***sla-iterator***— Name of the SLA iterator profile.

Required Privilege Level
view

List of Sample Output
clear oam ethernet connectivity-fault-management sla-iterator- statistics on page 2636

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault

-management sla-iterator- statistics

user@switch> **clear oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator i1**

```
Iterator statistics entries cleared
```

clear oam ethernet connectivity-fault-management statistics

Syntax

```
clear oam ethernet connectivity-fault-management statistics
<interface ethernet-interface-name>
<level md-level>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Clear all statistics maintained by CFM.

Options

interface *ethernet-interface-name*—(Optional) Clear CFM statistics only for MEPs attached to the specified Ethernet physical interface.

level *level*—(Optional) Clear CFM statistics only for MEPs within CFM maintenance domains (MDs) of the specified level.

Required Privilege Level

clear

RELATED DOCUMENTATION

- show oam ethernet connectivity-fault-management interfaces | 2694
- show oam ethernet connectivity-fault-management path-database | 2702
- show oam ethernet connectivity-fault-management mip | 2712

List of Sample Output

clear oam ethernet connectivity-fault-management statistics on page 2638

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-

management statistics

```
user@host> clear oam ethernet connectivity-fault-management statistics
```

```
Cleared statistics of all CFM sessions
```

clear oam ethernet connectivity-fault-management continuity-measurement

Syntax

```
clear oam ethernet connectivity-fault-management continuity-measurement
maintenance-domain md-name
maintenance-association ma-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 11.1.

Description

For all routers that support IEEE 802.1ag OAM connectivity fault management (CFM), clear the existing continuity measurement and restart counting the operational uptime (that is, the total time during which CCM adjacency is active for a particular remote MEP.).

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

local-mep *local-mep-id*—(Optional) Display connectivity fault management information for the specified local MEP only.

remote-mep *remote-mep-id*—(Optional) Display connectivity fault management information for the specified remote MEP only.

Required Privilege Level

view

RELATED DOCUMENTATION

Managing Continuity Measurement Statistics | 216

Ethernet Interfaces User Guide for Routing Devices

List of Sample Output

clear oam ethernet connectivity-fault-management continuity-measurement on page 2641

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management continuity-measurement

`user@host>` **clear oam ethernet connectivity-fault-management continuity-measurement maintenance-domain md5 maintenance-association ma5 local-mep 100 remote-mep 102**

```
Continuity measurement restarted.
```

clear oam ethernet connectivity-fault-management linktrace path-database

Syntax

clear oam ethernet connectivity-fault-management linktrace path-database mac-address maintenance-association ***ma-name*** **maintenance-domain** ***md-name***

Release Information

Command introduced in Junos OS Release 9.0.

Description

Clear all the linktrace entries and the relevant path information from the database for a particular remote host on M320, MX Series, T320, and T640 routers.

Options

mac-address—Clear connectivity fault management path database information for the specified MAC address of the remote host.

maintenance-association ***ma-name***—Clear connectivity fault management path database information for the specified maintenance association.

maintenance-domain ***md-name***—Clear connectivity fault management path database information for the specified maintenance domain.

Required Privilege Level

view

Sample Output

clear oam ethernet connectivity-fault-management linktrace path-database

`user@host>` **clear oam ethernet connectivity-fault-management linktrace path-database maintenance-domain md1 maintenance-association ma3 00058573e483**

```
This command produces no output.
```

clear oam ethernet connectivity-fault-management loss-statistics

Syntax

```
clear oam ethernet connectivity-fault-management loss-statistics
<interface ethernet-interface-name>
<level md-level>
```

Release Information

Command introduced in Junos OS Release 11.1.

Description

For all routers that support IEEE 802.1ag OAM connectivity fault management (CFM), clear all loss statistics maintained by CFM for a given maintenance domain and maintenance association.

In addition, for Ethernet interfaces on MX Series routers , clear any ITU-T Y.1731 Ethernet frame loss measurement (ETH-LM) statistics.

By default, the command clears ETH-LM statistics for CFM maintenance association end points (MEPs) attached to any interface on the router.

Options

interface *ethernet-interface-name*—(Optional) Clear ETH-LM statistics and ETH-LM frame counts only for MEPs attached to the specified Ethernet physical interface.

level *md-level*—(Optional) Clear ETH-LM statistics and ETH-LM frame counts only for MEPs within CFM maintenance domains (MDs) of the specified level.

Required Privilege Level

view

RELATED DOCUMENTATION

- Clearing ETH-LM Statistics | 226
- Displaying ETH-LM Statistics | 225
- Managing ETH-LM Statistics | 224

List of Sample Output

clear oam ethernet connectivity-fault-management loss-statistics on page 2644

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management loss-statistics

```
user@host> clear oam ethernet connectivity-fault-management loss-statistics

Cleared loss measurements statistics of all CFM sessions
```

clear oam ethernet connectivity-fault-management policer

Syntax

clear oam ethernet connectivity-fault-management policer maintenance-domain *md-name* maintenance-association *ma-name*

Release Information

Command introduced in Junos OS Release 10.0.

Description

On M7i and M10i with the Enhanced CFEB (CFEB-E), M320, M120, MX Series, T320, and T640 routers, clear connectivity-fault-management policer statistics.

Options

The following options are supported:

maintenance-domain md-name—Name of an existing CFM maintenance domain. If this option is not specified, policer statistics are cleared for all maintenance associations for all maintenance domains.

maintenance-association ma-name —Name of an existing CFM maintenance association. If this option is not specified, policer statistics are cleared for all maintenance associations for given maintenance domain. This option cannot be specified without specifying maintenance-domain name.

Required Privilege Level

view

RELATED DOCUMENTATION

show oam ethernet connectivity-fault-management policer | 2782

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear oam ethernet connectivity-fault-management policer

```
user@host> clear oam ethernet connectivity-fault-management policer
```

```
Policer statistics cleared
```

clear oam ethernet connectivity-fault-management policer maintenance-domain md-name maintenance-association ma-name

```
user@host> clear oam ethernet connectivity-fault-management policer
maintenance-domain md5 maintenance-association ma5-1
```

```
Policer statistics cleared
```

clear oam ethernet connectivity-fault-management statistics

Syntax

```
clear oam ethernet connectivity-fault-management statistics
<interface ethernet-interface-name>
<level md-level>
```

Release Information

Command introduced in Junos OS Release 8.4.
Support for ETH-DM statistics and frame counts added in Junos OS Release 9.5.

Description

For all routers that support IEEE 802.1ag OAM connectivity-fault management (CFM), clear all statistics maintained by CFM.

In addition, for Ethernet interfaces on Dense Port Concentrators (DPCs) in MX Series routers only, also clear any ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM) statistics and ETH-DM frame counts.

By default, the command clears CFM statistics and ETH-DM statistics and frame counts for CFM maintenance association end points (MEPs) attached to any interface on the router.

Options

ethernet-interface-name—(Optional) Clear CFM statistics, ETH-DM statistics, and ETH-DM frame counts only for MEPs attached to the specified Ethernet physical interface.

level—(Optional) Clear CFM statistics, ETH-DM statistics, and ETH-DM frame counts only for MEPs within CFM maintenance domains (MDs) of the specified level.

Required Privilege Level

view

RELATED DOCUMENTATION

- show oam ethernet connectivity-fault-management delay-statistics | 2679
- show oam ethernet connectivity-fault-management interfaces | 2727
- show oam ethernet connectivity-fault-management mep-database | 2749
- show oam ethernet connectivity-fault-management mep-statistics | 2764

List of Sample Output

clear oam ethernet connectivity-fault-management statistics on page 2648

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management statistics

```
user@host> clear oam ethernet connectivity-fault-management statistics

Cleared statistics of all CFM sessions
```

clear oam ethernet connectivity-fault-management synthetic-loss-measurement

Syntax

```
clear oam ethernet connectivity-fault-management synthetic-loss-measurement
maintenance-domain md-name
maintenance-association ma-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 13.2 for MX Series routers.

Description

(MX Series routers)—For all routers that support IEEE 802.1ag OAM connectivity fault management (CFM), clear the existing on-demand Ethernet synthetic loss measurement (ETH-SLM) statistics and restart counting the ETH-SLM frame counts and statistics.

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

local-mep *local-mep-id*—(Optional) Clear connectivity fault management information for the specified local MEP only.

remote-mep *remote-mep-id*—(Optional) Clear connectivity fault management information for the specified remote MEP only.

Required Privilege Level

view

RELATED DOCUMENTATION

monitor ethernet synthetic-loss-measurement | 2669

show oam ethernet connectivity-fault-management synthetic-loss-statistics | 2799

List of Sample Output

clear oam ethernet connectivity-fault-management synthetic-loss-measurement on page 2650

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management synthetic-loss-measurement

```
user@host> clear oam ethernet connectivity-fault-management synthetic-loss-measurement
maintenance-domain md5 maintenance-association ma5 local-mep 100 remote-mep 102
```

```
Synthetic loss measurement restarted.
```

monitor ethernet delay-measurement

Syntax

```
monitor ethernet delay-measurement maintenance-domain md-name maintenance-association ma-name (one-way
    | two-way) (remote-mac-address | mep remote-mep-id) <count count> <no-session-id-tlv> <priority 802.1p value>
    <size size> <wait time>
```

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.

Description

Start an ITU-T Y.1731 Ethernet frame delay measurement session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a summary of the frames exchanged in the measurement session. Frame delay measurement statistics are stored at one of the MEPs for later retrieval.

> **NOTE:** If you attempt to monitor delays to a nonexistent MAC address, you must type Ctrl +C to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

To start an Ethernet frame delay measurement session, the switch initiates an exchange of frames carrying one-way or two-way frame delay measurement protocol data units (PDUs) between the local and remote MEPs. The frame counts—the types of and number of Ethernet frame delay measurement PDU frames exchanged to measure frame delay times—are displayed as the run-time output of the **monitor ethernet delay-measurement** command and are also stored at both the initiator and receiver MEPs for later retrieval. Ethernet frame delay measurement statistics, described below, are measured and stored at only one of the MEPs:

Frame delay—The difference, in microseconds, between the time a frame is sent and when it is received.

Frame delay variation—The difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.”

For one-way Ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics.

Options

count *count*—(Optional) Number of frames to send to the specified peer MEP. The range of values is 1 through 65,535 frames. The default value is 10 frames.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

mep *remote-mep-id*—Numeric identifier of the peer MEP with which to perform Ethernet frame delay measurement. The discovered MAC address of the peer MEP is used. The range of values is 1 through 8191.

no-session-id-tlv—(Optional) Prevent insertion of the session ID TLV in the request frame.

one-way—Measurement type is one-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a one-way delay measurement request (1DM) frame and the time at which the receiver MEP receives the frame.

priority *802.1p value*—(Optional) Priority of the delay measurement request frame supported by both one-way delay measurement and two-way delay measurement. The range of values is from 0 through 7. The default value is zero.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet frame delay measurement. Specify the MAC address as six hexadecimal bytes in ***nn*:*nn*:*nn*:*nn*:*nn*:*nn*** format. Multicast MAC addresses are not supported.

size *size* —(Optional) Size of the data TLV to be included in the request frame. The range of values is from 1 through 1400 bytes.

two-way—Measurement type is two-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a two-way delay measurement message (DMM) frame and the time at which the initiator MEP receives an associated two-way delay measurement reply (DMR) frame from the responder MEP, subtracting the time elapsed at the responder MEP.

wait *time*—(Optional) Number of seconds to wait between sending frames. The range of values is from 1 through 255 seconds. The default value is 1 second.

Required Privilege Level
trace and maintenance

RELATED DOCUMENTATION

Configuring an Iterator Profile on a Switch (CLI Procedure) | 341

show oam ethernet connectivity-fault-management mep-database | 2705

show oam ethernet connectivity-fault-management mep-statistics | 2764

show oam ethernet connectivity-fault-management delay-statistics | 2679

clear oam ethernet connectivity-fault-management statistics | 2638

List of Sample Output

monitor ethernet delay-measurement one-way on page 2654
monitor ethernet delay-measurement two-way on page 2655
monitor ethernet delay-measurement two-way (Invalid DMR Frames Received) on page 2655

Output Fields

The **monitor ethernet delay-measurement** command displays different output at the CLI, depending on whether you start a one-way or two-way frame delay measurement:

- Table 224 on page 2653 lists the run-time output fields for the **monitor ethernet delay-measurement one-way** command.
- Table 225 on page 2654 lists the run-time output fields for the **monitor ethernet delay-measurement two-way** command.

Output fields are listed in the approximate order in which they appear.

Table 224: monitor ethernet delay-measurement one-way Output Fields

Output Field Name	Output Field Description
One-way ETH-DM request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
1DM Frames sent	PDU frames sent to the remote MEP in this ETH-DM session.
Packets transmitted	Total number of 1DM PDU frames sent to the remote MEP during this measurement session.
Average delay	Average two-way frame delay measured in this session.
Average delay variation	Average frame jitter measured in this session.
Best case delay	Lowest two-way frame delay measured in this session.
Worst case delay	Highest two-way frame delay measured in this session.
NOTE: For one-way delay measurement, these CLI output fields display **NA** (“not applicable”) at the initiator MEP because one-way frame delay measurements occur at the receiver MEP.	

Table 225: monitor ethernet delay-measurement two-way Output Fields

Output Field Name	Output Field Description
Two-way Ethernet frame delay measurement request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
DMR received from	Unicast MAC address of the remote MEP that transmitted this DMR frame in response to a DMM frame.
Delay	Two-way delay, in microseconds, for the initiator-transmitted DMM frame.
Delay variation	Difference, in microseconds, between the current and previous delay values. This is also known as *jitter*.
Packets transmitted	Total number of DMM PDU frames sent to the remote MEP in this measurement session.
Valid packets received	Total number of DMR PDU frames received from the remote MEP in this measurement session.
Average delay	Average two-way frame delay measured in this session.
Average delay variation	Average frame jitter measured in this session.
Best case delay	Lowest two-way frame delay measured in this session.
Worst case delay	Highest two-way frame delay measured in this session.

Sample Output

monitor ethernet delay-measurement one-way

`user@switch>` **monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
```

```
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

monitor ethernet delay-measurement two-way

`user@switch>` **monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a  Delay: 100 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 111 usec  Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a  Delay: 110 usec  Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a  Delay: 119 usec  Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a  Delay: 122 usec  Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 108 usec  Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

monitor ethernet delay-measurement two-way (Invalid DMR Frames Received)

`user@switch>` **monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a  Delay: 100 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 111 usec  Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a  Delay: 110 usec  Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a  Delay: 119 usec  Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a  Delay: 122 usec  Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a with invalid timestamp(s).
DMR received from 00:05:85:73:39:4a  Delay: 108 usec  Delay variation: 16 usec
```

```
--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 9, Invalid packets received: 1
Average delay: 105 usec, Average delay variation: 9 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

monitor ethernet delay-measurement

Syntax

```
monitor ethernet delay-measurement
maintenance-domain md-name
maintenance-association ma-name
(one-way | two-way)
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<local-mep mep-id>
<wait interval-seconds>
<priority 802.1p value>
<size>
<no-session-id-tlv>
<xml>
```

Release Information

Command introduced in Junos OS Release 9.5.
local-mep option introduced in Junos OS Release 15.1.

Description

Start an ITU-T Y.1731 Ethernet frame delay measurement session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a summary of the frames exchanged in the measurement session. Frame delay measurement statistics are stored at one of the MEPs for later retrieval.

> **NOTE:** If you attempt to monitor delays to a nonexistent MAC address, you must type Ctrl +c to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

To start an Ethernet frame delay measurement session, the router initiates an exchange of frames carrying one-way or two-way frame delay measurement protocol data units (PDUs) between the local and remote MEPs. The frame counts—the types of and number of Ethernet frame delay measurement PDU frames exchanged to measure frame delay times—are displayed as the runtime output of the **monitor ethernet delay-measurement** command and are also stored at both the initiator and receiver MEPs for later retrieval. Ethernet frame delay measurement statistics, described below, are measured and stored at only one of the MEPs:

Frame delay—The difference, in microseconds, between the time a frame is sent and when it is received.

Frame delay variation—The difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.”

For one-way Ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics.

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

one-way—Measurement type is one-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a one-way delay measurement request (1DM) frame and the time at which the receiver MEP receives the frame.

two-way—Measurement type is two-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a two-way delay measurement message (DMM) frame and the time at which the initiator MEP receives an associated two-way delay measurement reply (DMR) frame from the responder MEP, subtracting the time elapsed at the responder MEP.

mep *remote-mep-id*—Numeric identifier of the peer MEP with which to perform Ethernet frame delay measurement. The discovered MAC address of the peer MEP is used. The range of values is 1 through 8191.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet frame delay measurement. Specify the MAC address as six hexadecimal bytes in one of the following formats: ***nnnn.nnnn.nnnn*** or ***nn:nn:nn:nn:nn:nn***. For example, **0011.2233.4455** or **00:11:22:33:44:55**. Multicast MAC addresses are not supported.

count *frame-count*—(Optional) Number of frames to send to the specified peer MEP. The range of values is 1 through 65,535 frames. The default value is 10 frames.

local-mep *mep-id*—(Required when multiple MEPs are configured) Identifier for the local maintenance association end point.

wait *interval-seconds*—(Optional) Number of seconds to wait between sending frames. The range of values is from 1 through 255 seconds. The default value is 1 second.

priority *802.1p value*—(Optional) Priority of the delay measurement request frame supported by both one-way delay measurement and two-way delay measurement. The range of values is from 0 through 7. The default value is zero.

size—(Optional) Size of the data TLV to be included in the request frame. The range of values is from 1 through 1400 bytes.

no-session-id-tlv—(Optional) Prevent insertion of the session ID TLV in the request frame.

xml—(Optional) Allow the output of the command to be displayed in XML format supported by both one-way delay measurement and two-way delay measurement. Note that the only way to get output in XML format is to use the **xml** argument. The **display xml** command does not work.

Additional Information

To display the frame counts collected at an MEP as the result of this command, see the following command descriptions in the CLI Explorer:

- **show oam ethernet connectivity-fault-management interfaces detail**
- **show oam ethernet connectivity-fault-management mep-database**
- **show oam ethernet connectivity-fault-management mep-statistics**

To display the statistics collected at an MEP as the result of this command, see the following command descriptions in the CLI Explorer.

- **show oam ethernet connectivity-fault-management delay-statistics**
- **show oam ethernet connectivity-fault-management mep-statistics**

To clear both the frame counts and the statistics collected for MEPs, use the **clear oam ethernet connectivity-fault-management statistics** command, described in the CLI Explorer.

For a complete description of Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.

Required Privilege Level

trace and maintenance

List of Sample Output

monitor ethernet delay-measurement one-way on page 2661
monitor ethernet delay-measurement two-way on page 2661
monitor ethernet delay-measurement two-way (Invalid DMR Frames Received) on page 2662

Output Fields

The **monitor ethernet delay-measurement** command displays different output at the CLI, depending on whether you start a one-way or two-way frame delay measurement:

- Table 226 on page 2660 lists the run-time output fields for the **monitor ethernet delay-measurement one-way** command.
- Table 227 on page 2660 lists the run-time output fields for the **monitor ethernet delay-measurement two-way** command.

Output fields are listed in the approximate order in which they appear.

Table 226: monitor ethernet delay-measurement one-way Output Fields

Output Field Name	Output Field Description
One-way ETH-DM request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
1DM Frames sent	PDU frames sent to the remote MEP in this ETH-DM session.
Packets transmitted	Total number of 1DM PDU frames sent to the remote MEP during this measurement session.
Average delay	Average two-way frame delay measured in this session.
Average delay variation	Average frame jitter measured in this session.
Best case delay	Lowest two-way frame delay measured in this session.
Worst case delay	Highest two-way frame delay measured in this session.
NOTE: For one-way delay measurement, these CLI output fields display **NA** (“not applicable”) at the initiator MEP because one-way frame delay measurements occur at the receiver MEP.	

Table 227: monitor ethernet delay-measurement two-way Output Fields

Output Field Name	Output Field Description
Two-way Ethernet frame delay measurement request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
DMR received from	Unicast MAC address of the remote MEP that transmitted this DMR frame in response to a DMM frame.
Delay	Two-way delay, in microseconds, for the initiator-transmitted DMM frame.
Delay variation	Difference, in microseconds, between the current and previous delay values. This is also known as frame jitter.
Packets transmitted	Total number of DMM PDU frames sent to the remote MEP in this measurement session.

Table 227: monitor ethernet delay-measurement two-way Output Fields *(continued)*

Output Field Name	Output Field Description
Valid packets received	Total number of DMR PDU frames received from the remote MEP in this measurement session.
Average delay	Average two-way frame delay measured in this session.
Average delay variation	Average frame jitter measured in this session.
Best case delay	Lowest two-way frame delay measured in this session.
Worst case delay	Highest two-way frame delay measured in this session.

Sample Output

monitor ethernet delay-measurement one-way

`user@host>` **monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

monitor ethernet delay-measurement two-way

`user@host>` **monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a  Delay: 100 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 111 usec  Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a  Delay: 110 usec  Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a  Delay: 119 usec  Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a  Delay: 122 usec  Delay variation: 3 usec
```

```
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 108 usec  Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

monitor ethernet delay-measurement two-way (Invalid DMR Frames Received)

`user@host>` **monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10**

```
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a  Delay: 100 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a  Delay: 111 usec  Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a  Delay: 110 usec  Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a  Delay: 119 usec  Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a  Delay: 122 usec  Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a  Delay: 92 usec   Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a with invalid timestamp(s).
DMR received from 00:05:85:73:39:4a  Delay: 108 usec  Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 9, Invalid packets received: 1
Average delay: 105 usec, Average delay variation: 9 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

monitor ethernet loss-measurement

Syntax

```
monitor ethernet loss-measurement
maintenance-domain md-name
maintenance-association ma-name
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<local-mep mep-id>
<wait interval-seconds>
<priority 802.1p value>
<no-session-id-tlv>
<xml>
```

Release Information

Command introduced in Junos OS Release 11.1.
local-mep option introduced in Junos OS Release 15.1

Description

Start an ITU-T Y.1731 Ethernet frame loss measurement session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a count of transmitted and received data frames between the pair of MEPs. Frame loss measurement statistics are stored at one of the MEPs for later retrieval. For MX Series routers, supports point-to-point down MEPs for Ethernet interfaces (as per IEEE 802.1ag over VPWS).

> **NOTE:** If you attempt to monitor loss to a nonexistent MAC address, you must type Ctrl + c to explicitly quit the **monitor ethernet loss-measurement** command and return to the CLI command prompt.

To start an Ethernet frame loss measurement session, the router first sends frames with ETH-LM information to a peer MEP and similarly receives frames with ETH-LM information from the peer MEP. Frame loss is calculated by collecting the counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the **monitor ethernet loss-measurement** command and are also stored at the initiator. The frames counts are stored at both the initiator and the receiver MEPs for later retrieval.

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

mep *remote-mep-id*—Numeric identifier of the peer MEP with which to perform Ethernet frame loss measurement. The discovered MAC address of the peer MEP is used. The range of values is from 1 through 8192.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet frame loss measurement. Specify the MAC address as six hexadecimal bytes in one of the following formats: ***nnnn.nnnn.nnnn*** or ***nn:nn:nn:nn:nn:nn*** (for example, **0011.2233.4455** or **00:11:22:33:44:55**). Multicast MAC addresses are not supported.

count *frame-count*—(Optional) Number of frames to send to the specified peer MEP. The range of values is from 1 through 65535 frames. The default value is 10 frames.

local-mep *mep-id*—(Required when multiple MEPs are configured) Identifier for the local maintenance endpoint.

wait *interval-seconds*—(Optional) Number of seconds to wait between sending frames. The range of values is from 1 through 255 seconds. The default value is 1 second.

priority *802.1p value*—(Optional) Priority of the delay measurement request frame. The range of values is from 0 through 7. The default value is 1 second.

no-session-id-tlv—(Optional) Disable the **session id TLV** argument set in the request frame.

xml—(Optional) Allow the output of the command to be displayed in XML format.

Additional Information

To display the interator output for an LM session, run the following command:

- **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator <profile> maintenance-association <MA> maintenance-domain <MD> local-mep <MEP> remote-mep <RMEP>**

To display the frame counts collected at an MEP as the result of this command, see the following command descriptions in the CLI Explorer:

- **show oam ethernet connectivity-fault-management loss-statistics**
- **show oam ethernet connectivity-fault-management interfaces detail**
- **show oam ethernet connectivity-fault-management mep-database**
- **show oam ethernet connectivity-fault-management mep-statistics**

To display the statistics collected at an MEP as the result of this command, see the following command descriptions in the CLI Explorer:

- **show oam ethernet connectivity-fault-management delay-statistics**
- **show oam ethernet connectivity-fault-management mep-statistics**

To clear both the frame counts and the statistics collected for MEPs, use the **clear oam ethernet connectivity-fault-management loss-statistics maintenance-domain *md-name* maintenance-association *ma-name*** command, as described in the CLI Explorer.

For a complete description of Ethernet frame loss measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.

Required Privilege Level
trace and maintenance

RELATED DOCUMENTATION

- Ethernet Frame Loss Measurement Overview | **172**
- *Junos OS Network Interfaces Library for Routing Devices*
- CLI Explorer

List of Sample Output
monitor ethernet loss-measurement on page 2667

Output Fields
Table 228 on page 2665 lists the output fields for the **monitor ethernet loss-measurement** command and their descriptions. Output fields are listed in the approximate order in which they appear.

Table 228: monitor ethernet loss-measurement output fields

Output Field Name	Output Field Description
Ethernet loss delay measurement request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
LMR received from	Unicast MAC address of the remote MEP that transmitted this LMR frame in response to a loss measurement message (LMM) frame.
Near-end frame loss	Count of frame loss associated with ingress data frames.
Far-end frame loss	Count of frame loss associated with egress data frames.
Near-end loss ratio	Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the ingress interface.
Far-end loss ratio	Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the egress interface.

Table 228: monitor ethernet loss-measurement output fields *(continued)*

Output Field Name	Output Field Description
LMM packets transmitted	Total number of LMM PDU frames sent to the remote MEP in this measurement session.
LMR packets received	Total number of LMR PDU frames received from the remote MEP in this measurement session.
Average near-end frame loss	Average frame loss measured in this session associated with ingress data frames.
Average near-end loss ratio	Average frame loss ratio measured in this session associated with ingress data frames.
Average far-end frame loss	Average frame loss measured in this session associated with egress data frames.
Average far-end loss ratio	Average frame loss ratio measured in this session associated with egress data frames.
Near-end best case frame loss	Lowest frame loss measured in this session associated with ingress data frames.
Near-end best case loss ratio	Lowest frame loss ratio measured in this session associated with ingress data frames.
Near-end worst case frame loss	Highest frame loss measured in this session associated with ingress data frames.
Near-end worst case loss ratio	Highest frame loss ratio measured in this session associated with ingress data frames.
Far-end best case frame loss	Lowest frame loss measured in this session associated with egress data frames.
Far-end best case loss ratio	Lowest frame loss ratio measured in this session associated with egress data frames.
Far-end worst case frame loss	Highest frame loss measured in this session associated with egress data frames.
Far-end worst case loss ratio	Highest frame loss ratio measured in this session associated with egress data frames.

Note that in the preceding table, the term *number of service frames not delivered* is the difference between the number of service frames arriving at the ingress Ethernet flow point and the number of service frames delivered at the egress Ethernet flow point in a point-to-point Ethernet connection.

Sample Output

monitor ethernet loss-measurement

`user@host>` **monitor ethernet loss-measurement mep 2 64:87:88:6a:da:94 maintenance-domain md maintenance-association ma count 10**

```
ETH-LM request to 64:87:88:6a:da:94, Interface ge-2/3/2.0

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):0
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.00000%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):260
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.43537%

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):1
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.51546%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):257
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.31615%

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):0
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.00000%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):261
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.77551%

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):0
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.00000%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):260
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.43537%

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):1
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.51020%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):259
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.09524%
```

```
LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):0
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.00000%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):519
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.71795%

LMR received from 64:87:88:6a:da:94
Near-end frame loss(CIR)      :0           Far-end frame loss(CIR):1
Near-end frame loss ratio(CIR):0.00000% Far-end frame loss ratio(CIR):0.51020%
Near-end frame loss(EIR)      :0           Far-end frame loss(EIR):259
Near-end frame loss ratio(EIR):0.00000% Far-end frame loss ratio(EIR):88.09524%

--- Loss measurement statistics ---
LMM packets transmitted: 10, Valid LMR packets received: 8
Average near-end loss(CIR)         : 0.00000
Average near-end loss ratio(CIR)   : 0.00000%
Average far-end loss(CIR)          : 0.42857
Average far-end loss ratio(CIR)    : 0.21941%
Near-end best case loss(CIR)       : 0
Near-end best case loss ratio(CIR) : 0.00000%
Near-end worst case loss(CIR)      : 0
Near-end worst case loss ratio(CIR): 0.00000%
Far-end best case loss(CIR)        : 0
Far-end best case loss ratio(CIR)  : 0.00000%
Far-end worst case loss(CIR)       : 1
Far-end worst case loss ratio(CIR) : 0.51546%
Average near-end loss(EIR)         : 0.00000
Average near-end loss ratio(EIR)   : 0.00000%
Average far-end loss(EIR)          : 296.42857
Average far-end loss ratio(EIR)    : 88.41011%
Near-end best case loss(EIR)       : 0
Near-end best case loss ratio(EIR) : 0.00000%
Near-end worst case loss(EIR)      : 0
Near-end worst case loss ratio(EIR): 0.00000%
Far-end best case loss(EIR)        : 257
Far-end best case loss ratio(EIR)  : 88.09524%
Far-end worst case loss(EIR)       : 519
Far-end worst case loss ratio(EIR) : 88.77551%
```

monitor ethernet synthetic-loss-measurement

Syntax

```
monitor ethernet synthetic-loss-measurement
maintenance-domain md-name
maintenance-association ma-name
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<local-mep mep-id>
<wait interval-milliseconds>
<priority 802.1p value>
<size>
<xml>
```

Release Information

Command introduced in Junos OS Release 13.2 for MX Series routers.
local-mep option introduced in Junos OS Release 15.1

Description

(MX Series routers) Start an ITU-T Y.1731 Ethernet synthetic loss measurement (ETH-SLM) session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a summary of the frames exchanged in the measurement session. ETH-SLM (also called synthetic frame loss measurement) statistics are stored at one of the MEPs for later retrieval.

NOTE: If you attempt to monitor delays to a nonexistent MAC address, you must press Ctrl +c to explicitly quit the **monitor ethernet synthetic-loss-measurement** command and return to the CLI command prompt.

To start an Ethernet synthetic frame loss measurement session, the router initiates an exchange of frames carrying synthetic frame loss measurement protocol data units (PDUs) between the local and remote MEPs. The frame counts—the types of and number of Ethernet synthetic frame loss measurement PDU frames exchanged to measure frame delay times—are displayed as the run-time output of the **monitor ethernet synthetic-loss-measurement** command and are also stored at both the initiator and receiver MEPs for later retrieval. Ethernet synthetic frame loss measurement statistics, described below, are measured and stored at only one of the MEPs:

Frame delay—The difference, in microseconds, between the time a frame is sent and when it is received.

Frame delay variation—The difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.”

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

mep *remote-mep-id*—Numeric identifier of the peer MEP with which to perform Ethernet synthetic frame loss measurement. The discovered MAC address of the peer MEP is used. The range of values is from 1 through 8191.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet synthetic frame loss measurement. Specify the MAC address as six hexadecimal bytes in one of the following formats: ***nnnn.nnnn.nnnn*** or ***nn:nn:nn:nn:nn:nn***. For example, **0011.2233.4455** or **00:11:22:33:44:55**. Multicast MAC addresses are not supported.

count *frame-count*—(Optional) Number of frames to send to the specified peer MEP. The range of values is from 1 through 65,535 frames. The default value is 10 frames.

local-mep *mep-id*—(Required when multiple MEPs are configured) Identifier for the local maintenance endpoint.

wait *interval-milliseconds*—(Optional) Number of milliseconds to wait between sending frames. You must specify this value in multiples of 100 milliseconds. The range of values is from 100 through 50000 milliseconds. The default value is 100 milliseconds.

priority *802.1p value*—(Optional) Priority of the ETH-SLM request frame supported. The range of values is from 0 through 7. The default value is zero.

size—(Optional) Size of the data TLV to be included in the request frame. The range of values is from 1 through 1400 bytes.

xml—(Optional) Allow the output of the command to be displayed in XML format for ETH-SLM. Note that the only way to get output in XML format is to use the **xml** argument. The **display xml** command does not work.

Additional Information

To display the frame counts collected at a MEP as the result of this command, use the following commands as described in the CLI Explorer:

- **show oam ethernet connectivity-fault-management interfaces detail**
- **show oam ethernet connectivity-fault-management mep-database**
- **show oam ethernet connectivity-fault-management mep-statistics**

To display the statistics collected at a MEP as the result of this command, use the following commands as described in the CLI Explorer.

- **show oam ethernet connectivity-fault-management synthetic-loss-measurement**
- **show oam ethernet connectivity-fault-management mep-statistics**

To clear both the frame counts and the statistics collected for MEPs, use the **clear oam ethernet connectivity-fault-management statistics** command, described in the CLI Explorer.

For a complete description of Ethernet synthetic frame loss measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.

Required Privilege Level
trace and maintenance

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management synthetic-loss-measurement | **2649**

monitor ethernet synthetic-loss-measurement | **2669**

show oam ethernet connectivity-fault-management loss-statistics | **2744**

List of Sample Output
monitor ethernet synthetic-loss-measurement on page 2672

Output Fields

The **monitor ethernet synthetic-loss-measurement** command displays different output at the CLI, depending on when you start a synthetic frame loss measurement:

- Table 229 on page 2672 lists the run-time output fields for the **monitor ethernet synthetic-loss-measurement** command.

Output fields are listed in the approximate order in which they appear.

Table 229: monitor ethernet synthetic-loss-measurement Output Fields

Output Field Name	Output Field Description
ETH-SLM request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames received by the source MEP from the remote MEP during this measurement session.
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

monitor ethernet synthetic-loss-measurement

```
user@host> monitor ethernet synthetic-loss-measurement 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
```

```
ETH-SLM request to 00:05:85:73:39:4a, interface ge-1/0/0.0
      Synthetic Loss measurement statistics:
       SLM packets sent                          : 100
       SLR packets received                      : 100
       Accumulated SLM statistics:
       Local TXFC1 value                         : 100
       Local RXFC1 value                         : 100
       Last Received SLR frame TXFCf(tc)         : 100
       Last Received SLR frame TXFCb(tc)         : 100
       SLM Frame Loss:
       Frame Loss (far-end)                      : 0 (0.00 %)
       Frame Loss (near-end)                     : 0 (0.00 %)
```

monitor ethernet synthetic-loss-measurement

Syntax

```
monitor ethernet synthetic-loss-measurement
maintenance-domain md-name
maintenance-association ma-name
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<local-mep mep-id>
<wait interval-milliseconds>
<priority 802.1p value>
<size>
<xml>
```

Release Information

Command introduced in Junos OS Release 13.2 for MX Series routers.
local-mep option introduced in Junos OS Release 15.1

Description

(MX Series routers) Start an ITU-T Y.1731 Ethernet synthetic loss measurement (ETH-SLM) session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a summary of the frames exchanged in the measurement session. ETH-SLM (also called synthetic frame loss measurement) statistics are stored at one of the MEPs for later retrieval.

NOTE: If you attempt to monitor delays to a nonexistent MAC address, you must press Ctrl +c to explicitly quit the **monitor ethernet synthetic-loss-measurement** command and return to the CLI command prompt.

To start an Ethernet synthetic frame loss measurement session, the router initiates an exchange of frames carrying synthetic frame loss measurement protocol data units (PDUs) between the local and remote MEPs. The frame counts—the types of and number of Ethernet synthetic frame loss measurement PDU frames exchanged to measure frame delay times—are displayed as the run-time output of the **monitor ethernet synthetic-loss-measurement** command and are also stored at both the initiator and receiver MEPs for later retrieval. Ethernet synthetic frame loss measurement statistics, described below, are measured and stored at only one of the MEPs:

Frame delay—The difference, in microseconds, between the time a frame is sent and when it is received.

Frame delay variation—The difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.”

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

mep *remote-mep-id*—Numeric identifier of the peer MEP with which to perform Ethernet synthetic frame loss measurement. The discovered MAC address of the peer MEP is used. The range of values is from 1 through 8191.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet synthetic frame loss measurement. Specify the MAC address as six hexadecimal bytes in one of the following formats: ***nnnn.nnnn.nnnn*** or ***nn:nn:nn:nn:nn:nn***. For example, **0011.2233.4455** or **00:11:22:33:44:55**. Multicast MAC addresses are not supported.

count *frame-count*—(Optional) Number of frames to send to the specified peer MEP. The range of values is from 1 through 65,535 frames. The default value is 10 frames.

local-mep *mep-id*—(Required when multiple MEPs are configured) Identifier for the local maintenance endpoint.

wait *interval-milliseconds*—(Optional) Number of milliseconds to wait between sending frames. You must specify this value in multiples of 100 milliseconds. The range of values is from 100 through 50000 milliseconds. The default value is 100 milliseconds.

priority *802.1p value*—(Optional) Priority of the ETH-SLM request frame supported. The range of values is from 0 through 7. The default value is zero.

size—(Optional) Size of the data TLV to be included in the request frame. The range of values is from 1 through 1400 bytes.

xml—(Optional) Allow the output of the command to be displayed in XML format for ETH-SLM. Note that the only way to get output in XML format is to use the **xml** argument. The **display xml** command does not work.

Additional Information

To display the frame counts collected at a MEP as the result of this command, use the following commands as described in the CLI Explorer:

- **show oam ethernet connectivity-fault-management interfaces detail**
- **show oam ethernet connectivity-fault-management mep-database**
- **show oam ethernet connectivity-fault-management mep-statistics**

To display the statistics collected at a MEP as the result of this command, use the following commands as described in the CLI Explorer.

- **show oam ethernet connectivity-fault-management synthetic-loss-measurement**
- **show oam ethernet connectivity-fault-management mep-statistics**

To clear both the frame counts and the statistics collected for MEPs, use the **clear oam ethernet connectivity-fault-management statistics** command, described in the CLI Explorer.

For a complete description of Ethernet synthetic frame loss measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.

Required Privilege Level
trace and maintenance

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management synthetic-loss-measurement | 2649

monitor ethernet synthetic-loss-measurement | 2669

show oam ethernet connectivity-fault-management loss-statistics | 2744

List of Sample Output
monitor ethernet synthetic-loss-measurement on page 2677

Output Fields

The **monitor ethernet synthetic-loss-measurement** command displays different output at the CLI, depending on when you start a synthetic frame loss measurement:

- Table 229 on page 2672 lists the run-time output fields for the **monitor ethernet synthetic-loss-measurement** command.

Output fields are listed in the approximate order in which they appear.

Table 230: monitor ethernet synthetic-loss-measurement Output Fields

Output Field Name	Output Field Description
ETH-SLM request to	Unicast MAC address of the remote peer MEP.
Interface	Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames received by the source MEP from the remote MEP during this measurement session.
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

monitor ethernet synthetic-loss-measurement

```
user@host> monitor ethernet synthetic-loss-measurement 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
```

```
ETH-SLM request to 00:05:85:73:39:4a, interface ge-1/0/0.0
      Synthetic Loss measurement statistics:
       SLM packets sent                          : 100
       SLR packets received                      : 100
       Accumulated SLM statistics:
       Local TXFC1 value                         : 100
       Local RXFC1 value                         : 100
       Last Received SLR frame TXFCf(tc)         : 100
       Last Received SLR frame TXFCb(tc)         : 100
       SLM Frame Loss:
       Frame Loss (far-end)                      : 0 (0.00 %)
       Frame Loss (near-end)                     : 0 (0.00 %)
```

show oam ethernet connectivity-fault-management delay-statistics

Syntax

```
show oam ethernet connectivity-fault-management delay-statistics
<count entry-count>
<local-mep mep-id>
<maintenance-association ma-name>
<maintenance-domain md-name>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 11.4 for EX Series switches.

Description

On MX Series routers with Ethernet interfaces on Dense Port Concentrators (DPCs), display ETH-DM delay statistics.

On EX Series switches, display delay measurement results.

Options

count *entry-count*—(Optional) Number of entries to display from the statistics table. The range of values is **1** through **100**. The default value is **100** entries.

local-mep *mep-id*—(Optional) Numeric identifier of the local MEP. On MX Series routers, the range of values is **1** through **8192**. On EX Series switches, the range of values is **1** through **8191**.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

maintenance-domain *md-name*—Name of an existing connectivity fault management (CFM) maintenance domain.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. On MX Series routers, the range of values is **1** through **8192**. On EX Series switches, the range of values is **1** through **8191**.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | **2647**

clear oam ethernet connectivity-fault-management delay-statistics | **2634**

show oam ethernet connectivity-fault-management interfaces | 2727
show oam ethernet connectivity-fault-management mep-database | 2749
show oam ethernet connectivity-fault-management mep-statistics | 2764

List of Sample Output

show oam ethernet connectivity-fault-management delay-statistics on page 2681
show oam ethernet connectivity-fault-management delay-statistics remote-mep on page 2682

Output Fields

Table 231 on page 2680 lists the output fields for the **show oam ethernet connectivity-fault-management delay-statistics** command and the **show oam ethernet connectivity-fault-management mep-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 231: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields

Output Field Name	Field Description
MEP identifier	Maintenance association end point (MEP) numeric identifier.
MAC address	Unicast MAC address configured for the MEP.
Remote MEP count	Number of remote MEPs (unless you specify the **remote-mep** option).
Remote MEP identifier	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Index	Index number that corresponds to the ETH-DM entry in the CFM database.
One-way delay (usec)	For a one-way ETH-DM session, the frame delay time, in microseconds, measured at the receiver MEP. For a detailed description of one-way Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.
Two-way delay (usec)	For a two-way ETH-DM session, the frame delay time, in microseconds, measured at the initiator MEP. For a detailed description of two-way Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.
Average one-way delay	Average one-way frame delay for the statistics displayed.

Table 231: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields *(continued)*

Output Field Name	Field Description
Average one-way delay variation	Average one-way “frame jitter” for the statistics displayed.
Best-case one-way delay	Lowest one-way frame delay for the statistics displayed.
Worst-case one-way delay	Highest one-way frame delay for the statistics displayed.
Average two-way delay	Average two-way frame delay for the statistics displayed.
Average two-way delay variation	Average two-way “frame jitter” for the statistics displayed.
Best-case two-way delay	Lowest two-way frame delay for the statistics displayed.
Worst-case two-way delay	Highest two-way frame delay calculated in this session.

Sample Output

show oam ethernet connectivity-fault-management delay-statistics

`user@switch>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md6 maintenance-association ma6**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count: 2
  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        259            519
      2        273            550
      3        287            571
      4        299            610
      5        313            650
    Average one-way delay          : 286 usec
    Average one-way delay variation: 62 usec
    Best case one-way delay        : 259 usec
```

```
    Worst case one-way delay       : 313 usec
    Average two-way delay          : 580 usec
    Average two-way delay variation: 26 usec
    Best case two-way delay        : 519 usec
    Worst case two-way delay       : 650 usec

  Remote MEP identifier: 102
  Remote MAC address: 00:04:55:63:39:5a
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        29             58
      2        23             59
      3        27             56
      4        29             62
      5        33             68
    Average one-way delay          : 28 usec
    Average one-way delay variation: 3 usec
    Best case one-way delay        : 23 usec
    Worst case one-way delay       : 33 usec
    Average two-way delay          : 60 usec
    Average two-way delay variation: 3 usec
    Best case two-way delay        : 56 usec
    Worst case two-way delay       : 68 usec
```

show oam ethernet connectivity-fault-management delay-statistics remote-mep

`user@switch>` **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md6 maintenance-association ma6 remote-mep 101**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39

  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        259            519
      2        273            550
      3        287            571
      4        299            610
      5        313            650
    Average one-way delay          : 286 usec
```

```
Average one-way delay variation: 62 usec
Best case one-way delay        : 259 usec
Worst case one-way delay       : 313 usec
Average two-way delay          : 580 usec
Average two-way delay variation: 26 usec
Best case two-way delay        : 519 usec
Worst case two-way delay       : 650 usec
```

show oam ethernet connectivity-fault-management forwarding-state

Syntax

```
show oam ethernet connectivity-fault-management forwarding-state
interface interface-name | instance instance-name
<brief | detail | extensive>
```

Release Information

Command introduced in Junos OS Release 8.4.

Description

On M7i and M10i with the Enhanced CFEB (CFEB-E), M320, MX Series, T320, and T640 routers, display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management forwarding state information for Ethernet interfaces.

Options

interface *interface-name*—Display forwarding state information for the specified Ethernet interface only.

instance *instance-name*—Display forwarding state information for the specified forwarding instance only.

brief | detail | extensive—(Optional) Display the specified level of output.

Required Privilege Level

view

List of Sample Output

show oam ethernet connectivity-fault-management forwarding-state instance on page 2685
show oam ethernet connectivity-fault-management forwarding-state interface on page 2686
show oam ethernet connectivity-fault-management forwarding-state interface detail on page 2686
show oam ethernet connectivity-fault-management forwarding-state interfaceinterface-name on page 2688

Output Fields

Table 232 on page 2684 lists the output fields for the **show oam ethernet connectivity-fault-management forwarding-state** command. Output fields are listed in the approximate order in which they appear.

Table 232: show oam ethernet connectivity-fault-management forwarding-state Output Fields

Field Name	Field Description	Level of Output
Interface name	Interface identifier.	All levels
Link (Status)	Local link status.	All levels
Filter action	Filter action for messages at the level.	All levels

Table 232: show oam ethernet connectivity-fault-management forwarding-state Output Fields *(continued)*

Field Name	Field Description	Level of Output
Next hop type	Next-hop type.	All levels
Next index	Next-hop index number.	**brief**
Level	Maintenance domain (MD) level.	**detail**
Direction	MEP direction configured.	none
Instance name	Forwarding instance name.	All levels
CEs	Number of customer edge (CE) interfaces.	All levels
VEs	Number of VPN endpoint (VE) interfaces.	All levels

Sample Output

show oam ethernet connectivity-fault-management forwarding-state instance

`user@host>` **show oam ethernet connectivity–fault-management forwarding-state instance**

```
Instance name: __+bd1__
CEs: 3
VEs: 0
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7                       Drop              none
```

show oam ethernet connectivity-fault-management forwarding-state interface

```
user@host> show oam ethernet connectivity-fault-management forwarding-state interface
```

```
Interface name: ge-3/0/0.0
Instance name: __+bd1__
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none

Interface name: xe-0/0/0.0
Instance name: __+bd1__
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none
```

show oam ethernet connectivity-fault-management forwarding-state interface detail

```
user@host> show oam ethernet connectivity-fault-management forwarding-state interface detail
```

```
Interface name: ge-3/0/0.0
Instance name: __+bd1__
```

```
  Level: 0
  Filter action: Drop
  Nexthop type: none

  Level: 1
  Filter action: Drop
  Nexthop type: none

  Level: 2
  Filter action: Drop
  Nexthop type: none

  Level: 3
  Filter action: Drop
  Nexthop type: none

  Level: 4
  Filter action: Drop
  Nexthop type: none

  Level: 5
  Filter action: Drop
  Nexthop type: none

  Level: 6
  Filter action: Drop
  Nexthop type: none

  Level: 7
  Direction: down
  Filter action: Receive
  Nexthop type: none

Interface name: xe-0/0/0.0
Instance name: __+bd1__

  Level: 0
  Filter action: Drop
  Nexthop type: none

  Level: 1
  Filter action: Drop
  Nexthop type: none
```

```
...
```

show oam ethernet connectivity-fault-management forwarding-state interface interface-name

`user@host>` **show oam ethernet connectivity-fault-management forwarding-state interface interface-name ge-3/0/0/0.0**

```
Interface name: ge-3/0/0.0
Instance name: __+bd1__
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none
```

show oam ethernet connectivity-fault-management forwarding-state

Syntax

```
show oam ethernet connectivity-fault-management forwarding-state
interface interface-name
<brief | detail | extensive>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management forwarding state information for Ethernet interfaces.

Options

interface *interface-name*—Display forwarding state information for the specified Ethernet interface only.

brief | detail | extensive—(Optional) Display the specified level of output.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2638

show oam ethernet connectivity-fault-management path-database | 2702

show oam ethernet connectivity-fault-management mip | 2712

List of Sample Output

show oam ethernet connectivity-fault-management forwarding-state on page 2690
show oam ethernet connectivity-fault-management forwarding-state interface on page 2690
show oam ethernet connectivity-fault-management forwarding-state interface detail on page 2691
show oam ethernet connectivity-fault-management forwarding-state interface interface-name on page 2692

Output Fields

Table 232 on page 2684 lists the output fields for the **show oam ethernet connectivity-fault-management forwarding-state** command. Output fields are listed in the approximate order in which they appear.

Table 233: show oam ethernet connectivity-fault-management forwarding-state Output Fields

Field Name	Field Description	Level of Output
Interface name	Interface identifier.	All levels
Filter action	Filter action for messages at the level.	All levels
Nexthop type	Next-hop type.	All levels
Nexthop index	Next-hop index number.	**brief**
Level	Maintenance domain (MD) level.	**detail**
Direction	MEP direction configured.	none
CEs	Number of customer edge (CE) interfaces.	All levels

Sample Output

show oam ethernet connectivity-fault-management forwarding-state

```
user@host> show oam ethernet connectivity–fault-management forwarding-state
```

```
CEs: 3

  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7                       Drop              none
```

show oam ethernet connectivity-fault-

management forwarding-state interface

user@host> **show oam ethernet connectivity-fault-management forwarding-state interface**

```
Interface name: ge-3/0/0.0
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none

Interface name: xe-0/0/0.0
Instance name: __+bd1__
  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none
```

show oam ethernet connectivity-fault-management forwarding-state interface detail

user@host> **show oam ethernet connectivity-fault-management forwarding-state interface detail**

```
Interface name: ge-3/0/0.0

  Level: 0
  Filter action: Drop
  Nexthop type: none
```

```
  Level: 1
  Filter action: Drop
  Nexthop type: none

  Level: 2
  Filter action: Drop
  Nexthop type: none

  Level: 3
  Filter action: Drop
  Nexthop type: none

  Level: 4
  Filter action: Drop
  Nexthop type: none

  Level: 5
  Filter action: Drop
  Nexthop type: none

  Level: 6
  Filter action: Drop
  Nexthop type: none

  Level: 7
  Direction: down
  Filter action: Receive
  Nexthop type: none

Interface name: xe-0/0/0.0

  Level: 0
  Filter action: Drop
  Nexthop type: none

  Level: 1
  Filter action: Drop
  Nexthop type: none

  ...
```

show oam ethernet connectivity-fault-management forwarding-

state interface
interface-name

user@host> **show oam ethernet connectivity-fault-management forwarding-state interface interface-name ge-3/0/0.0**

```
Interface name: ge-3/0/0.0

  Maintenance domain forwarding state:

  Level    Direction      Filter action     Nexthop      Nexthop
                                            type         index
  0                       Drop              none
  1                       Drop              none
  2                       Drop              none
  3                       Drop              none
  4                       Drop              none
  5                       Drop              none
  6                       Drop              none
  7        down           Receive           none
```

show oam ethernet connectivity-fault-management interfaces

Syntax

```
show oam ethernet connectivity-fault-management interfaces
<ethernet-interface-name>
<level md-level>
<brief | detail | extensive>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for Ethernet interfaces.

Options

brief | detail | extensive—(Optional) Display the specified level of output.

ethernet-interface-name—(Optional) Display CFM information only for CFM entities attached to the specified Ethernet interface.

level *md-level*—(Optional) Display CFM information for CFM identities enclosed within a maintenance domain of the specified level.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2638

show oam ethernet connectivity-fault-management path-database | 2702

show oam ethernet connectivity-fault-management mip | 2712

List of Sample Output

show oam ethernet connectivity-fault-management interfaces on page 2698
show oam ethernet connectivity-fault-management interfaces detail on page 2698
show oam ethernet connectivity-fault-management interfacesextensive on page 2699
show oam ethernet connectivity-fault-management interfaces level on page 2700
show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces) on page 2701

Output Fields

Table 234 on page 2695 lists the output fields for the **show oam ethernet connectivity-fault-management interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 234: show oam ethernet connectivity-fault-management interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Interface identifier.	All levels
Interface status	Local interface status.	All levels
Link status	Local link status. **Up**, **down**, or **oam-down**.	All levels
Maintenance domain name	Maintenance domain name.	**detail extensive**
Format (Maintenance domain)	Maintenance domain name format configured.	**detail extensive**
Level	Maintenance domain level configured.	All levels
Maintenance association name	Maintenance association name.	**detail extensive**
Format (Maintenance association)	Maintenance association name format configured.	**detail extensive**
Continuity-check status	Continuity-check status.	**detail extensive**
Interval	Continuity-check message interval.	**detail extensive**
Loss-threshold	Lost continuity-check message threshold.	**detail extensive**
MEP identifier	Maintenance association end point (MEP) identifier.	All levels
Neighbours	Number of MEP neighbors.	All levels
Direction	MEP direction configured.	**detail extensive**
MAC address	MAC address configured for the MEP.	**detail extensive**
MEP status	Indicates the status of the Connectivity Fault Management (CFM) protocol running on the MEP: **Running**, **inactive**, **disabled**, or **unsupported**.	**detail extensive**

Table 234: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote MEP not receiving CCM	Whether the remote MEP is not receiving connectivity check messages (CCMs).	**detail extensive**
Erroneous CCM received	Whether erroneous CCMs have been received.	**detail extensive**
Cross-connect CCM received	Whether cross-connect CCMs have been received.	**detail extensive**
RDI sent by some MEP	Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.	**detail extensive**
CCMs sent	Number of CCMs transmitted.	**detail extensive**
CCMs received out of sequence	Number of CCMs received out of sequence.	**detail extensive**
LBMs sent	Number of loopback request messages (LBMs) sent.	**detail extensive**
Valid in-order LBRs received	Number of loopback response messages (LBRs) received that were valid messages and in sequence.	**detail extensive**
Valid out-of-order LBRs received	Number of LBRs received that were valid messages and not in sequence.	**detail extensive**
LBRs received with corrupted data	Number of LBRs received that were corrupted.	**detail extensive**
LBRs sent	Number of LBRs transmitted.	**detail extensive**
LTMs sent	Linktrace messages (LTMs) transmitted.	**detail extensive**
LTMs received	Linktrace messages received.	**detail extensive**
LTRs sent	Linktrace responses (LTRs) transmitted.	**detail extensive**
LTRs received	Linktrace responses received.	**detail extensive**

Table 234: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sequence number of next LTM request	Sequence number of next LTM request to be transmitted.	**detail extensive**
1DMs sent	If the interface is attached to an initiator MEP for a one-way ETH-DM session: Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.	**detail extensive**
Valid 1DMs received	If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of valid 1DM frames received. For all other cases, this field displays **0**.	**detail extensive**
Invalid 1DMs received	If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of invalid 1DM frames received. For all other cases, this field displays **0**.	**detail extensive**
DMMs sent	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.	**detail extensive**
DMRs sent	If the interface is attached to a responder MEP for a two-way ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays **0**.	**detail extensive**
Valid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays **0**.	**detail extensive**
Invalid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays **0**.	**detail extensive**
Remote MEP count	Number of remote MEPs.	**extensive**

Table 234: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Identifier (remote MEP)	MEP identifier of the remote MEP.	**extensive**
MAC address (remote MEP)	MAC address of the remote MEP.	**extensive**
State (remote MEP)	State of the remote MEP.	**extensive**
Interface (remote MEP)	Interface of the remote MEP.	**extensive**

Sample Output

show oam ethernet connectivity-fault-management interfaces

```
user@host> show oam ethernet connectivity-fault-management interfaces
```

```
Interface       Link       Status          Level       MEP          Neighbours
                                                       Identifier
ge-1/1/0.0      Up         Active          0           2            1
ge-1/1/0.1      Up         Active          0           2            1
ge-1/1/0.10     Up         Active          0           2            1
ge-1/1/0.100    Up         Active          0           2            1
ge-1/1/0.101    Up         Active          0           2            1
ge-1/1/0.102    Up         Active          0           2            1
ge-1/1/0.103    Up         Active          0           2            1
ge-1/1/0.104    Up         Active          0           2            1
ge-1/1/0.105    Up         Active          0           2            1
ge-1/1/0.106    Up         Active          0           2            1

...
```

show oam ethernet connectivity-fault-management interfaces detail

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
```

```
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Maintenance domain name: md0, Format: string, Level: 5
    Maintenance association name: ma1, Format: string
    Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
    MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : yes
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : yes
    Statistics:
      CCMs sent                                    : 76
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
      LBRs received with corrupted data            : 0
      LBRs sent                                    : 0
      LTMs sent                                    : 0
      LTMs received                                : 0
      LTRs sent                                    : 0
      LTRs received                                : 0
      Sequence number of next LTM request          : 1320235363
      1DMs sent                                    : 0
      Valid 1DMs received                          : 0
      Invalid 1DMs received                        : 0
      DMMs sent                                    : 0
      DMRs sent                                    : 0
      Valid DMRs received                          : 0
      Invalid DMRs received                        : 0
    Remote MEP count: 2
      Identifier    MAC address        State    Interface
       2001     00:90:69:0b:7f:71       ok    ge-5/2/9.0
       4001     00:90:69:0b:09:c5       ok    ge-5/2/9.0
```

show oam ethernet connectivity-fault-management interfaces extensive

user@host> **show oam ethernet connectivity-fault-management interfaces extensive**

```
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Maintenance domain name: md0, Format: string, Level: 5
```

```
Maintenance association name: ma1, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM                 : no
  Erroneous CCM received                       : yes
  Cross-connect CCM received                   : no
  RDI sent by some MEP                         : yes
Statistics:
  CCMs sent                                    : 76
  CCMs received out of sequence                : 0
  LBMs sent                                    : 0
  Valid in-order LBRs received                 : 0
  Valid out-of-order LBRs received             : 0
  LBRs received with corrupted data            : 0
  LBRs sent                                    : 0
  LTMs sent                                    : 0
  LTMs received                                : 0
  LTRs sent                                    : 0
  LTRs received                                : 0
  Sequence number of next LTM request          : 1542035464
  1DMs sent                                    : 0
  Valid 1DMs received                          : 0
  Invalid 1DMs received                        : 0
  DMMs sent                                    : 0
  DMRs sent                                    : 0
  Valid DMRs received                          : 0
  Invalid DMRs received                        : 0
Remote MEP count: 2
  Identifier    MAC address        State    Interface
   2001     00:90:69:0b:7f:71       ok    ge-5/2/9.0
   4001     00:90:69:0b:09:c5       ok    ge-5/2/9.0
```

show oam ethernet connectivity-fault-management interfaces level

user@host> **show oam ethernet connectivity-fault-management interfaces level 7**

```
Interface       Link       Status          Level       MEP          Neighbours
                                                       Identifier
ge-3/0/0.0      Up         Active          7           201          0
xe-0/0/0.0      Up         Active          7           203          1
```

show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces)

user@host> **show oam ethernet connectivity-fault-management interfaces**

```
Interface                  Link      Status       Level  MEP         Neighbours
                                                       Identifier
ge-4/0/1.0, vlan 100       Up        Active       5      100         0
ge-10/3/10.4091, vlan 4091 Down      Inactive     4      400         0
ge-4/0/0.0                 Up        Active       6      200         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-4/0/0.0**

```
Interface                  Link      Status       Level  MEP         Neighbours
                                                       Identifier
ge-4/0/0.0                 Up        Active       6      200         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-4/0/1.0 vlan 100**

```
Interface                  Link      Status       Level  MEP         Neighbours
                                                       Identifier
ge-4/0/1.0, vlan 100       Up        Active       5      100         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-10/3/10.4091 vlan 4091**

```
Interface                  Link      Status       Level  MEP         Neighbours
                                                       Identifier
ge-10/3/10.4091, vlan 4091 Down      Inactive     4      400         0
```

show oam ethernet connectivity-fault-management path-database

Syntax

show oam ethernet connectivity-fault-management path-database *host* **maintenance-association** *ma-name* **maintenance-domain** *md-name mac-address*

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management maintenance linktrace database information.

Options

mac-address—Display connectivity fault management path database information for the specified MAC address of the remote host.

maintenance-association ***ma-name***—Display connectivity fault management path database information for the specified maintenance association.

maintenance-domain ***md-name***—Display connectivity fault management path database information for the specified maintenance domain.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2638

show oam ethernet connectivity-fault-management interfaces | 2694

show oam ethernet connectivity-fault-management mip | 2712

List of Sample Output

show oam ethernet connectivity-fault-management path-database on page 2703
show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands) on page 2704

Output Fields

Table 235 on page 2703 lists the output fields for the **show oam ethernet connectivity-fault-management path-database** command. Output fields are listed in the approximate order in which they appear.

Table 235: show oam ethernet connectivity-fault-management linktrace path-database Output Fields

Field Name	Field Description
Linktrace to	MAC address of the 802.1ag node to which the linktrace message is targeted.
Interface	Interface used by the local MEP to send the linktrace message (LTM).
Maintenance Domain	Maintenance domain identifier specified in the traceroute command.
Maintenance Association	Maintenance association identifier specified in the traceroute command.
Level	Maintenance domain level configured for the maintenance domain.
Local Mep	MEP identifier of the local MEP originating the linktrace.
Hop	Sequential hop count of the linktrace path.
TTL	Number of hops remaining in the linktrace message (LTM). The time to live (TTL) is decremented at each hop.
Source MAC address	MAC address of the 802.1ag maintenance intermediate point (MIP) that is forwarding the LTM.
Next hop MAC address	MAC address of the 802.1ag node that is the next hop in the LTM path.
Transaction Identifier	4-byte identifier maintained by the MEP. Each LTM uses a transaction identifier. The transaction identifier is maintained globally across all maintenance domains. Use the transaction identifier to match an incoming linktrace responses (LTR), with a previously sent LTM.

Sample Output

show oam ethernet connectivity-fault-management path-database

```
user@host> show oam ethernet connectivity-fault-management path-database maintenance-domain MD1 maintenance-association MA1 00:01:02:03:04:05

Linktrace to 00:01:02:03:04:05, Interface : ge-5/0/0.0
       Maintenance Domain: MD1, Level: 7
       Maintenance Association: MA1, Local Mep: 1
```

```
       Hop     TTL      Source MAC address        Next hop MAC address
       Transaction Identifier:100001
       1       63       00:00:aa:aa:aa:aa         00:00:bb:bb:bb:bb
       2       62       00:00:bb:bb:bb:bb         00:00:cc:cc:cc:cc
       3       61       00:00:cc:cc:cc:cc         00:01:02:03:04:05
       4       60       00:01:02:03:04:05         00:00:00:00:00:00
```

show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands)

`user@host>` **show oam ethernet connectivity-fault-management path-database maintenance-domain MD2 maintenance-association MA2 00:06:07:08:09:0A**

```
Linktrace to 00:06:07:08:09:0A, Interface : ge-5/0/1.0
       Maintenance Domain: MD2, Level: 6
       Maintenance Association: MA2, Local Mep: 10

       Hop     TTL      Source MAC address        Next hop MAC address
       Transaction Identifier:100002
       1       63       00:00:aa:aa:aa:aa         00:00:bb:bb:bb:bb
       2       62       00:00:bb:bb:bb:bb         00:00:cc:cc:cc:cc
       3       61       00:00:cc:cc:cc:cc         00:06:07:08:09:0A
       4       60       00:06:07:08:09:0A         00:00:00:00:00:00
       Transaction Identifier:100003
       1       63       00:00:aa:aa:aa:aa         00:00:bb:bb:bb:bb
       2       62       00:00:bb:bb:bb:bb         00:00:cc:cc:cc:cc
       3       61       00:00:cc:cc:cc:cc         00:06:07:08:09:0A
       4       60       00:06:07:08:09:0A         00:00:00:00:00:00
```

show oam ethernet connectivity-fault-management mep-database

Syntax

```
show oam ethernet connectivity-fault-management mep-database
maintenance-domain domain-name
maintenance-association ma-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

Options

maintenance-association *ma-name*—Display connectivity fault management information for the specified maintenance association.

maintenance-domain *domain-name*—Display connectivity fault management information for the specified maintenance domain.

local-mep *local-mep-id*—(Optional) Display connectivity fault management information for the specified local MEP only.

remote-mep *remote-mep-id*—(Optional) Display connectivity fault management information for the specified remote MEP only.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2638

show oam ethernet connectivity-fault-management interfaces | 2694

show oam ethernet connectivity-fault-management mip | 2712

List of Sample Output

show oam ethernet connectivity-fault-management mep-database on page 2709

show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 2710

show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event) on page 2710

Output Fields

Table 236 on page 2706 lists the output fields for the **show oam ethernet connectivity-fault-management mep-database** command. Output fields are listed in the approximate order in which they appear.

Table 236: show oam ethernet connectivity-fault-management mep-database Output Fields

Field Name	Field Description
Maintenance domain name	Maintenance domain name.
Format (Maintenance domain)	Maintenance domain name format configured.
Level	Maintenance domain level configured.
Maintenance association name	Maintenance association name.
Format (Maintenance association)	Maintenance association name format configured.
Continuity-check status	Continuity-check status.
Interval	Continuity-check message interval.
MEP identifier	Maintenance association end point (MEP) identifier.
Direction	MEP direction configured.
MAC address	MAC address configured for the MEP.
Auto-discovery	Whether automatic discovery is enabled or disabled.
Priority	Priority used for CCMs and linktrace messages transmitted by the MEP.
Interface name	Interface identifier.
Interface status	Local interface status.
Link status	Local link status.

Table 236: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
Remote MEP not receiving CCM	Whether the remote MEP is not receiving CCMs.
Erroneous CCM received	Whether erroneous CCMs have been received.
Cross-connect CCM received	Whether cross-connect CCMs have been received.
RDI sent by some MEP	Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.
CCMs sent	Number of CCMs transmitted.
CCMs received out of sequence	Number of CCMs received out of sequence.
LBMs sent	Number of loopback messages (LBMs) sent.
Valid in-order LBRs received	Number of loopback response messages (LBRs) received that were valid messages and in sequence.
Valid out-of-order LBRs received	Number of LBRs received that were valid messages and not in sequence.
LBRs received with corrupted data	Number of LBRs received that were corrupted.
LBRs sent	Number of LBRs transmitted.
LTMs sent	Linktrace messages (LTMs) transmitted.
LTMs received	Linktrace messages received.
LTRs sent	Linktrace responses (LTRs) transmitted.
LTRs received	Linktrace responses received.
Sequence number of next LTM request	Sequence number of the next linktrace message request to be transmitted.

Table 236: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
1DMs sent	If the MEP is an initiator for a one-way ETH-DM session: Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.
Valid 1DMs received	If the MEP is a receiver for a one-way ETH-DM session: Number of valid 1DM frames received. For all other cases, this field displays **0**.
Invalid 1DMs received	If the MEP is a receiver for a one-way ETH-DM session: Number of invalid 1DM frames received. For all other cases, this field displays **0**.
DMMs sent	If the MEP is an initiator for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.
DMRs sent	If the MEP is a responder for a ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays **0**.
Valid DMRs received	If the MEP is an initiator for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays **0**.
Invalid DMRs received	If the MEP is an initiator for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays **0**.
Remote MEP identifier	MEP identifier of the remote MEP.
State (remote MEP)	State of the remote MEP: **idle**, **start**, **ok**, or **failed**.
MAC address	MAC address of the remote MEP.
Type	Whether the remote MEP MAC address was learned using automatic discovery or configured.
Interface	Interface of the remote MEP. A seven-digit number is appended if CFM is configured to run on a routing instance of type VPLS.

Table 236: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
Last flapped	Date, time, and how long ago the remote MEP interface went from down to up. The format is **Last flapped: *year-month-day hours:minutes:seconds timezone* (*hours:minutes:seconds* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.
Remote defect indication	Whether the remote defect indication (RDI) bit is set in messages that have been received or transmitted.
Port status TLV	• In the Maintenance domain section, displays the last transmitted port status TLV value. • In the Remote MEP section, displays the last value of port status TLV received from the remote MEP. In the Action profile section, displays, the last occurred event **port-status-tlv blocked** event. This event occurred due to the reception of **blocked** value in the port status TLV from remote MEP.
Interface status TLV	• In the Maintenance domain section, displays the last transmitted interface status TLV value. • In the Remote MEP section, displays the last value of interface status TLV received from the remote MEP. In the Action profile section, if displays, the last occurred event interface-status-tlv event (either **lower-layer-down** or **down**). This event occurred due to the reception of either lower or **down** value in the interface status TLV from remote MEP.
Action profile	Name of the action profile occurrence associated with a remote MEP.
Last event	When an action profile occurs, displays the last event that triggered it.
Last event cleared	When all the configured and occurred events (under action profile) are cleared, then the action taken gets reverted (such as down interface is made up) and the corresponding time is noted and displayed.
Action	Action taken and the corresponding time of the action occurrence.

Sample Output

show oam ethernet connectivity-fault-management mep-database

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
vpls-vlan2000 maintenance-association vpls-vlan200
```

```
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
  Maintenance association name: vpls-vlan200, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                 : no
    Erroneous CCM received                       : no
    Cross-connect CCM received                   : no
    RDI sent by some MEP                         : no
  Statistics:
    CCMs sent                                    : 1476
    CCMs received out of sequence                : 0
    LBMs sent                                    : 85
    Remote MEP count: 1
    Identifier    MAC address        State    Interface
      100     00:19:e2:b2:81:4b       ok  vt-0/1/10.1049088
```

show oam ethernet connectivity-fault-management mep-database local-mep remote-mep

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200 local-mep 200 remote-mep 100**

```
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
  Maintenance association name: vpls-vlan200, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 100, State: ok
    MAC address: 00:19:e2:b2:81:4b, Type: Learned
    Interface: vt-0/1/10.1049088
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
```

show oam ethernet connectivity-fault-management mep-database remote-mep

(Action Profile Event)

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5 remote-mep 200**

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 200, State: ok
    MAC address: 00:05:85:73:96:1f, Type: Configured
    Interface: ge-1/0/8.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: lower-layer-down
    Action profile: juniper
      Last event: Interface-status-tlv lower-layer-down
      Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
```

show oam ethernet connectivity-fault-management mip

Syntax

```
show oam ethernet connectivity-fault-management mip
<qualifier>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display all the maintenance association intermediate points (MIPs) created in the system. Specify qualifiers to display specific MIPs.

Options

qualifier—(Optional) Display the specified MIP.

Required Privilege Level

view

RELATED DOCUMENTATION

- show oam ethernet connectivity-fault-management interfaces | 2694
- show oam ethernet connectivity-fault-management path-database | 2702

List of Sample Output

show oam ethernet connectivity-fault-management mip on page 2713

Output Fields

Table 237 on page 2712 lists the output fields for the **show oam ethernet connectivity-fault-management mip** command. Output fields are listed in the approximate order in which they appear.

Table 237: show oam ethernet connectivity-fault-management mip Output Fields

Field Name	Field Description
MIP information for instance	Header for the MIP information showing the MIP name.
Interface	Interface type-dpc/pic/port.unit-number.
Level	MIP level configured.

Sample Output

show oam ethernet connectivity-fault -management mip

```
user@host> show oam ethernet connectivity-fault-management mip
```

```
MIP information for  __mip_name__

MIP information for  default-switch bd1

  Interface       Level
  ge-3/0/0.0          7
  ge-3/0/1.0          6
  ge-3/0/3.0          6
```

show oam ethernet connectivity-fault-management sla-iterator-statistics

Syntax

```
show oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-domain md-name
maintenance-association ma-name
sla-iterator sla-iterator
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 9.6.
Command introduced in Junos OS Release 12.2 for ACX Series routers.
Command introduced in Junos OS Release 13.2 for MX Series routers (not on MPC3E Hyperion cards).

Description

Display the Ethernet Operation, Administration, and Maintenance (OAM) service-level agreement (SLA) iterator statistics.

Options

maintenance-domain *md-name*—Name of an existing connectivity fault management (CFM) maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

sla-iterator *sla-iterator*— Name of the iterator profile.

local-mep *local-mep-id*—(Optional) Numeric identifier of the local MEP. The range of values is **1** through **8191**.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. The range of values is **1** through **8192**.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring an Iterator Profile on a Switch (CLI Procedure) | **341**

clear oam ethernet connectivity-fault-management sla-iterator-statistics | **2636**

List of Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics on page 2718
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) on page 2718
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM)in Metro Ethernet Forum (MEF) mode on page 2720
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) in Metro Ethernet Forum (MEF) mode on page 2721
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay measurement (DM) statistics in non-Metro Ethernet Forum (MEF) mode on page 2723
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) statistics in non-Metro Ethernet Forum (MEF) mode on page 2723
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM) with “legacy-pm-display” option in enhanced-cfm mode on page 2724
show oam ethernet connectivity-fault-management state - To verify the Connectivity Fault Management (CFM) state on page 2725

Output Fields

Table 238 on page 2715 lists the output fields for the **show oam ethernet connectivity-fault-management sla-iterator-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 238: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields

Output Field Name	Output Field Description
Maintenance domain	Name of the maintenance domain.
Level	Level of the maintenance domain level configured.
Maintenance association	Name of the maintenance association.
Local MEP id	Numeric identifier of the local MEP.
Remote MEP id	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Iterator name	Name of iterator.
Iterator Id	Numeric identifier of the iterator.
Iterator cycle time	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
Iteration period	Maximum number of cycles per iteration
Iterator status	Current status of iterator whether running or stopped.

Table 238: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

Output Field Name	Output Field Description
Infinite iterations	Status of iteration as infinite or finite.
Counter reset time	Date and time when the counter was reset.
Reset reason	Reason to reset counter.
Delay weight	Calculation weight of delay.
Delay variation weight	Calculation weight of delay variation.
DMM sent	Delay measurement message (DMM) PDU frames sent to the peer MEP in this session.
DMM skipped for threshold hit	Number of DMM frames sent to the peer MEP in this session skipped during threshold hit.
DMM skipped for threshold hit window	Number of DMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
DMR received	Number of delay measurement reply (DMR) frames received.
DMR out of sequence	Total number of DMR out of sequence packets received.
DMR received with invalid time stamps	Total number of DMR frames received with invalid timestamps.
Average two-way delay	Average two-way frame delay for the statistics displayed.
Average two-way delay variation	Average two-way “frame jitter” for the statistics displayed.
Average one-way forward delay variation	Average one-way forward delay variation for the statistics displayed in microseconds.
Average one-way backward delay variation	Average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average two-way delay	Weighted average two-way delay for the statistics displayed in microseconds.
Weighted average two-way delay variation	Weighted average two-way delay variation for the statistics displayed in microseconds.

Table 238: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

Output Field Name	Output Field Description
Weighted average one-way backward delay variation	Weighted average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average one-way forward delay variation	Weighted average one-way forward delay variation for the statistics displayed in microseconds.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLM packets received	Total number of synthetic loss message (SLM) PDU frames that the remote MEP received from the source MEP during this ETH-SLM session.
SLR packets sent	Total number of synthetic loss reply (SLR) PDU frames that the remote MEP sent to the source MEP during this measurement session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames that the source MEP received from the remote MEP during this measurement session.
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

show oam ethernet connectivity-fault -management sla-iterator-statistics

user@switch> **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 2**

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i1, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap

Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent                                          : 23898520
DMM skipped for threshold hit                     : 11000
DMM skipped for threshold hit window              : 0
DMR received                                      : 23851165
DMR out of sequence                               : 1142
DMR received with invalid time stamps             : 36540
Average two-way delay                             : 129 usec
Average two-way delay variation                   : 15 usec
Average one-way forward delay variation           : 22 usec
Average one-way backward delay variation          : 22 usec
Weighted average two-way delay                    : 134 usec
Weighted average two-way delay variation          : 8 usec
Weighted average one-way forward delay variation  : 6 usec
Weighted average one-way backward delay variation : 2 usec
```

Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers)

user@router> **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain mdu maintenance-association mau local-mep 4 remote-mep 3 sla-iterator lm**

```
Iterator statistics:
  Maintenance domain: 2, Level: 2
  Maintenance association: W-160432000-001, Local MEP id: 2
  Remote MEP id: 1, Remote MAC address: 00:90:69:0a:43:39
  Iterator name: iter1, Iterator Id: 1
  Iterator cycle time: 100ms, Iteration period: 10 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2012-09-25 02:15:31 PDT (00:00:45 ago)
  Reset reason: Adjacency flap
  Iterator loss measurement statistics:
    LMM sent                            : 444
    LMM skipped for threshold hit       : 0
    LMM skipped for threshold hit window: 0
    LMR received                        : 444
    LMR out of sequence                 : 0
    LMR forwarding-class mismatch       : 0
  Accumulated transmit statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)                       : 0
  Accumulated receive statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)                       : 0
  Accumulated loss statistics:
    Near-end loss (CIR)                 : 0
    Near-end loss-ratio (CIR)           : 0 (0.00000%)
    Far-end loss (CIR)                  : 0
    Far-end loss-ratio (CIR)            : 0 (0.00000%)
    Near-end loss (CIR)                 : 0
    Near-end loss-ratio (EIR)           : 0 (0.00000%)
    Far-end loss (CIR)                  : 0
    Far-end loss-ratio (EIR)            : 0 (0.00000%)
  Last loss measurement statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)
```

Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM)in Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator DM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM, Iterator Id: 1
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:48:23 PST (00:00:54 ago)
  Reset reason: Adjacency flap
  Current delay measurement statistics:
    Measurement Interval Index                : 2 (Suspect status : 1)
    Measurement Interval Start Time           : 2018-12-05 19:48:23 PST (Elapsed
 time : 53011 msec)
    Frame Delay two way (min, max, avg)       : 251 , 295 , 262  (usec)
    Frame Delay forward (min, max, avg)       : 125 , 147 , 131  (usec)
    Frame Delay backward (min, max, avg)      : 125 , 147 , 131  (usec)
    Inter Frame Delay two way (min, max, avg) : 0 , 42 , 7  (usec)
    Inter Frame Delay forward (min, max, avg) : 0 , 21 , 3  (usec)
    Inter Frame Delay backward (min, max, avg) : 0 , 21 , 3  (usec)
    Frame Delay Range two way (max, avg)      : 0 , 0  (usec)
    Frame Delay Range forward (max, avg)      : 0 , 0  (usec)
    Frame Delay Range backward (max, avg)     : 0 , 0  (usec)
    SOAM TXed                                 : 52
    SOAM RXed                                 : 52

  Delay measurement bin statistics:
    Measurement Interval Index     : 2
    Two Way Frame Delay
       [0           - 4999       ] (usec)   : 52
       [5000        - 9999       ] (usec)   : 0
       [10000       - Infinity   ] (usec)   : 0
    Forward Frame Delay
       [0           - 4999       ] (usec)   : 52
       [5000        - 9999       ] (usec)   : 0
       [10000       - Infinity   ] (usec)   : 0
    Backward Frame Delay
       [0           - 4999       ] (usec)   : 52
```

```
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Two Way Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Forward Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Backward Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Two Way Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Forward Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Backward Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) in Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator SLM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_SLM, Iterator Id: 2
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:48:23 PST (00:00:11 ago)
  Reset reason: Adjacency flap
  Iterator synthetic loss measurement statistics:
```

```
   SLM skipped for threshold hit        : 0
   SLM skipped for threshold hit window : 0
   SLR out of sequence                  : 0
   SLM Sample Size                      : 180 SLMs
   Local packet Stats (TxFCl, RxFCl)    : 11, 11
   Last SLR packet stats (TxFCf, TxFCb) : 11, 11
   Last measured FLR (fwd, bkwd)        : 0.000%, 0.000% (Sample #NA)


 Current Measurement Interval loss statistics:
   Measurement Interval Index           : 2 (Suspect Status: 1)
   Measurement Interval Start Time      : 2018-12-05 19:48:23 PST (Elapsed time:
10042 msec)
   SOAM Frames (Tx, Rx)                 : 10, 10
   Forward Frame Stats (Tx, Rx)         : 10, 10
   Backward Frame Stats (Tx, Rx)        : 10, 10
   Frame Loss (fwd, bkwd)               : 0, 0
   Forward FLR minimum                  : 0.000%
   Forward FLR maximum                  : 0.000%
   Forward FLR average                  : 0.000%
   Backward FLR minimum                 : 0.000%
   Backward FLR maximum                 : 0.000%
   Backward FLR average                 : 0.000%

 Current Measurement Interval availability statistics:
   Measurement Interval Index           : 2 (Suspect Status: 1)
   Measurement Interval Start Time      : 2018-12-05 19:48:23 PST (Elapsed time:
10042 msec)
   High loss (fwd, bkwd)                : 0 , 0
   Consecutive high loss (fwd, bkwd)    : 0 , 0
   Available (fwd, bkwd)                : 0 , 0
   Unavailable (fwd, bkwd)              : 0 , 0
   Forward FLR minimum                  : 0.000%
   Forward FLR maximum                  : 0.000%
   Forward FLR average                  : 0.000%
   Backward FLR minimum                 : 0.000%
   Backward FLR maximum                 : 0.000%
   Backward FLR average                 : 0.000%

   Last known available status  (fwd, bkwd)    : unknown, unknown
   Last known forward availability transition  : NA
   Last known backward availability transition : NA
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay measurement (DM) statistics in non-Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator DM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM, Iterator Id: 1
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:43:47 PST (00:02:44 ago)
  Reset reason: Adjacency flap
  Iterator delay measurement statistics:
    Calculation weight: Delay: 1, Delay variation: 1
    DMM sent                                        : 164
    DMM skipped for threshold hit                   : 0
    DMM skipped for threshold hit window            : 0
    DMR received                                    : 164
    DMR out of sequence                             : 0
    DMR forwarding-class mismatch                   : 0
    DMR received with invalid time stamps           : 0
    Average two-way delay                           : 234 usec
    Average two-way delay variation                 : 9 usec
    Average one-way forward delay variation         : 346 usec
    Average one-way backward delay variation        : 346 usec
    Weighted average two-way delay                  : 221 usec
    Weighted average two-way delay variation        : 2 usec
    Weighted average one-way forward delay variation : 357 usec
    Weighted average one-way backward delay variation: 355 usec
    Bestcase two-way delay                          : 210 usec
    Worstcase two-way delay                         : 283 usec
    Weighted Bestcase two-way delay                 : 210 usec
    Weighted Worstcase two-way delay                : 283 usec
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) statistics in non-Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator SLM**

```
Iterator statistics:
```

```
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_SLM, Iterator Id: 2
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:43:47 PST (00:03:23 ago)
  Reset reason: Adjacency flap
  Iterator synthetic loss measurement statistics:
    SLM sent                            : 202
    SLM skipped for threshold hit       : 0
    SLM skipped for threshold hit window: 0
    SLR received                        : 202
    SLR out of sequence                 : 0
  SLM  transmit statistics:
    SLM TXed                            : 202
    SLM RXed                            : 202
    SLM Last packet Tx count            : 202
    SLM Last packet Rx count            : 202
  Last loss measurement statistics:
    Near-end loss                       : 0 (0.00%)
    Far-end  loss                       : 0 (0.00%)
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM) with “legacy-pm-display” option in enhanced-cfm mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator Legacy**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM_Legacy, Iterator Id: 3
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:51:33 PST (00:00:15 ago)
  Reset reason: Adjacency flap
  Iterator delay measurement statistics:
    Calculation weight: Delay: 1, Delay variation: 1
    DMM sent                                        : 14
    DMM skipped for threshold hit                   : 0
    DMM skipped for threshold hit window            : 0
```

```
    DMR received                                    : 14
    DMR out of sequence                             : 0
    DMR forwarding-class mismatch                   : 0
    DMR received with invalid time stamps           : 0
    Average two-way delay                           : 324 usec
    Average two-way delay variation                 : 7 usec
    Average one-way forward delay variation         : 240 usec
    Average one-way backward delay variation        : 240 usec
    Weighted average two-way delay                  : 324 usec
    Weighted average two-way delay variation        : 6 usec
    Weighted average one-way forward delay variation : 222 usec
    Weighted average one-way backward delay variation: 222 usec
    Bestcase two-way delay                          : 312 usec
    Worstcase two-way delay                         : 333 usec
    Weighted Bestcase two-way delay                 : 312 usec
    Weighted Worstcase two-way delay                : 333 usec
```

show oam ethernet connectivity-fault-management state - To verify the Connectivity Fault Management (CFM) state

The following command is to verify whether the CFM state is in enhanced-cfm mode or not.

`user@router>` **show oam ethernet connectivity-fault-management state**

```
Connectivity fault management state:
    CFM Mode Of Operation: Enhanced
    Enhanced IP Mode: Enabled
    CFM Config State: Ok
    CFM Cleanup State: Ok
    CFM Restart Timer State: Cleanup Timer State stopped Rebooting in 0 sec
    CFM CFMMAN Job State: Not Pending
    Number of sessions: 1
    Number of sessions created: 1
    Number of sessions deleted: 0
    Number of sessions freed: 0
    Number of sessions enqueued: 1
    Number of sessions dequeued: 1
    VPLS feature: enabled
    Token based forwarding feature: enabled
    Forwarding table filtering simulation feature: disabled
    Hardware assisted flooding feature: enabled
    Flood resynchronization for GRES feature: enabled
    Shared interface filter feature: disabled
    Hardware timestamping feature: disabled
```

```
    Marking of connection protection TLV feature: disabled
    CFMD config memory resource  limit(in bytes): 3221225472
    CFMD max resident set (peak) size (in bytes):  24158208

Packet processing state:
    State of the connection to packet processing daemon: down
    State of the flow to packet processing daemon: ready
    State of the packet processing job: ready
    Number of times the connection to packet processing daemon was blocked: 0
    State of the connection to cfmman: slots: 2 3 4 5

Filter state:
    State of the connection to firewall daemon: Connected
    Number of reconnects made to firewall daemon: 0
    Number of requests sent to firewall daemon: 13
    Number of requests accepted by firewall daemon: 13
    Number of requests rejected by firewall daemon: 0
    Number of requests lost due to disconnection: 0
```

show oam ethernet connectivity-fault-management interfaces

Syntax

```
show oam ethernet connectivity-fault-management interfaces
<ethernet-interface-name>
<level md-level>
<brief | detail | extensive>
```

Release Information

Command introduced in Junos OS Release 8.4.
Support for ITU-T Y.1731 frame delay measurement added in Junos OS Release 9.5.
Support for ITU-T Y.1731 Ethernet synthetic frame loss measurement (ETH-SLM) added in Junos OS Release 13.2 for ACX Series and MX Series routers.

Description

On M7i and M10i routers with Enhanced CFEB (CFEB-E), and on M320, MX Series, ACX Series, T320, and T640 routers, display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for Ethernet interfaces.

In addition, for Ethernet interfaces on MX Series routers , also display any ITU-T Y.1731 frame delay measurement (ETH-DM) frame counts when **detail** or **extensive** mode is specified.

For Ethernet interfaces on MX Series routers, display any ITU-T Y.1731 synthetic frame loss measurement (ETH-SLM) statistics and frame counts.

Options

brief | detail | extensive—(Optional) Specified level of output.

ethernet-interface-name—(Optional) CFM information only for CFM entities attached to the specified Ethernet interface.

level *md-level*—(Optional) CFM information for CFM identities enclosed within a maintenance domain of the specified level.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2647
show oam ethernet connectivity-fault-management delay-statistics | 2679
show oam ethernet connectivity-fault-management mep-database | 2749

show oam ethernet connectivity-fault-management mep-statistics | 2764

Ethernet Alarm Indication Signal (ETH-AIS) Function Overview | 286

List of Sample Output

show oam ethernet connectivity-fault-management interfaces on page 2734
show oam ethernet connectivity-fault-management interfaces detail on page 2734
show oam ethernet connectivity-fault-management interfaces detail (One-Way ETH-DM) on page 2735
show oam ethernet connectivity-fault-management interfaces detail(Connection Protection TLV Configured) on page 2736
show oam ethernet connectivity-fault-management interfacesextensive on page 2737
show oam ethernet connectivity-fault-management interfaces level on page 2739
show oam ethernet connectivity-fault-management interfaces (trunk ports) on page 2739

Output Fields

Table 234 on page 2695 lists the output fields for the **show oam ethernet connectivity-fault-management interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Interface identifier.	All levels
Interface status	Local interface status.	All levels
Link status	Local link status. **Up**, **down**, or **oam-down**.	All levels
Maintenance domain name	Maintenance domain name.	**detail extensive**
Format (Maintenance domain)	Maintenance domain name format configured.	**detail extensive**
Level	Maintenance domain level configured.	All levels
Maintenance association name	Maintenance association name.	**detail extensive**
Format (Maintenance association)	Maintenance association name format configured.	**detail extensive**
Continuity-check status	Continuity-check status.	**detail extensive**

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Ethernet-ais status	Status of alarm indication signal (AIS). **active** or **in-active**.	**detail extensive**
Interval	Continuity-check message interval.	**detail extensive**
Loss-threshold	Lost continuity-check message threshold.	**detail extensive**
Interface status TLV	Status of the interface status TLV, if configured on the MEP interface: **none**, **up**, **down**, **testing**, **unknown**, **dormant**, **notPresent**, **lowerLayerDown**	**detail extensive**
Port status TLV	Status of the port status TLV, if configured on the MEP interface: **none**, **no**, **yes**	**detail extensive**
Connection Protection TLV	Status of the connection protection TLV if configured on the MEP interface: **no**, **yes** If **yes**, then the transmitted connection protection TLV is decoded and the following three fields are displayed: **Prefer me**, **Protection in use**, **FRR Flag**	**detail extensive**
Prefer me	If set to **yes**, the path through which CCM was transmitted is preferred (unless the path fails). It is used for signaling a manual-switch command to the remote side. Its value can be **yes** or **no**.	**detail extensive**
Protection in use	Used for protection decision coordination. Its value is set to **yes** if the endpoint transmitting the CCM is currently transmitting the user traffic to protection path. Its value can be **yes** or **no**.	**detail extensive**
FRR Flag	LSR/LER forwarding the CCM Frame into a bypass tunnel is set. Its value can be **yes** or **no**.	**detail extensive**
MEP identifier	Maintenance association end point (MEP) identifier.	All levels
Neighbors	Number of MEP neighbors.	All levels
Direction	MEP direction configured.	**detail extensive**
MAC address	MAC address configured for the MEP.	**detail extensive**

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
MEP status	Indicates the status of the connectivity fault management (CFM) protocol running on the MEP: **Running**, **inactive**, **disabled**, or **unsupported**.	**detail extensive**
Remote MEP not receiving CCM	Whether the remote MEP is not receiving connectivity check messages (CCMs).	**detail extensive**
Erroneous CCM received	Whether erroneous CCMs have been received.	**detail extensive**
Cross-connect CCM received	Whether cross-connect CCMs have been received.	**detail extensive**
RDI sent by some MEP	Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.	**detail extensive**
Some remote MEP's MAC in error state	Indicates whether the remote MEP's MAC is in error state.	**detail extensive**
Alarm Indication Signal	Indicates whether the AIS is triggered or is cleared.	**detail extensive**
CCMs sent	Number of CCMs transmitted.	**detail extensive**
CCMs received out of sequence	Number of CCMs received out of sequence.	**detail extensive**
LBMs sent	Number of loopback request messages (LBMs) sent.	**detail extensive**
Valid in-order LBRs received	Number of loopback response messages (LBRs) received that were valid messages and in sequence.	**detail extensive**
Valid out-of-order LBRs received	Number of LBRs received that were valid messages and not in sequence.	**detail extensive**
LBRs received with corrupted data	Number of LBRs received that were corrupted.	**detail extensive**

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
LBRs sent	Number of LBRs transmitted.	**detail extensive**
LTMs sent	Linktrace messages (LTMs) transmitted.	**detail extensive**
LTMs received	Linktrace messages received.	**detail extensive**
LTRs sent	Linktrace responses (LTRs) transmitted.	**detail extensive**
LTRs received	Linktrace responses received.	**detail extensive**
Sequence number of next LTM request	Sequence number of next LTM request to be transmitted.	**detail extensive**
1DMs sent	If the interface is attached to an initiator MEP for a one-way ETH-DM session: Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.	**detail extensive**
Valid 1DMs received	If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of valid 1DM frames received. For all other cases, this field displays **0**.	**detail extensive**
Invalid 1DMs received	If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of invalid 1DM frames received. For all other cases, this field displays **0**.	**detail extensive**
Out of sync 1DMs received	If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of out-of-sync one-way delay measurement request packets received.	**detail extensive**
DMMs sent	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.	**detail extensive**
Valid DMMs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid two-way delay measurement request packets received.	**detail extensive**

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Invalid DMMs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of invalid two-way delay measurement request packets received.	**detail extensive**
DMRs sent	If the interface is attached to a responder MEP for a two-way ETH-DM session: Number of delay measurement reply (DMR) frames sent. For all other cases, this field displays **0**.	**detail extensive**
Valid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays **0**.	**detail extensive**
Invalid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays **0**.	**detail extensive**
LMM sent	If the interface is attached to an initiator MEP for a ETH-LM session: Number of loss measurement message (LMM) PDU frames sent to the peer MEP in this session.	**detail extensive**
Valid LMM received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of valid loss measurement request packets received.	**detail extensive**
Invalid LMM received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of invalid loss measurement request packets received.	**detail extensive**
LMR sent	If the interface is attached to a responder MEP for a ETH-LM session: Number of loss measurement reply (LMR) frames sent.	**detail extensive**
Valid LMR received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of valid LMR frames received.	**detail extensive**
Invalid LMR received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of invalid LMR frames received.	**detail extensive**
Valid AIS frames transmitted	Number of valid AIS frames transmitted to the peer MEPs.	**detail extensive**
Valid AIS frames received	Number of valid AIS frames received from the peer MEPs.	**detail extensive**

Table 239: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
SLM sent	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of synthetic loss measurement (SLM) request packets transmitted from the source MEP to the remote or destination MEP in this session.	**detail extensive**
Valid SLM received	If the interface is attached to a responder MEP for a ETH-SLM session: Number of valid SLM PDUs transmitted from the source MEP to the remote or destination MEP.	**detail extensive**
Invalid SLM received	If the interface is attached to a responder MEP for a ETH-SLM session: Number of invalid SLM PDUs transmitted from the source MEP to the remote or destination MEP.	**detail extensive**
SLR sent	If the interface is attached to a responder MEP for a ETH-SLM session: Number detail extensive of synthetic loss reply (SLR) frames sent.	**detail extensive**
Valid SLR received	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of valid SLR PDUs that the source MEP received from the remote or destination MEP.	**detail extensive**
Invalid SLR received	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of invalid SLR PDUs that the source MEP received from the remote or destination MEP.	**detail extensive**
Remote MEP count	Number of remote MEPs.	**extensive**
Identifier (remote MEP)	MEP identifier of the remote MEP.	**extensive**
MAC address (remote MEP)	MAC address of the remote MEP.	**extensive**
State (remote MEP)	State of the remote MEP.	**extensive**
Interface (remote MEP)	Interface of the remote MEP.	**extensive**

Sample Output

show oam ethernet connectivity-fault-management interfaces

```
user@host> show oam ethernet connectivity-fault-management interfaces
```

```
Interface       Link       Status           Level       MEP          Neighbors
                                                        Identifier
ge-1/1/0.0      Up         Active           0           2            1
ge-1/1/0.1      Up         Active           0           2            1
ge-1/1/0.10     Up         Active           0           2            1
ge-1/1/0.100    Up         Active           0           2            1
ge-1/1/0.101    Up         Active           0           2            1
ge-1/1/0.102    Up         Active           0           2            1
ge-1/1/0.103    Up         Active           0           2            1
ge-1/1/0.104    Up         Active           0           2            1
ge-1/1/0.105    Up         Active           0           2            1
ge-1/1/0.106    Up         Active           0           2            1

...
```

show oam ethernet connectivity-fault-management interfaces detail

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
```

```
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Maintenance domain name: md0, Format: string, Level: 5
  Maintenance association name: ma1, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
   MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : yes
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : yes
      Alarm Indication Signal                      : yes
    Statistics:
      CCMs sent                                    : 76
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
```

```
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 1320235363

      1DMs sent                                     : 0
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0
      LMM sent                                      : 10
      Valid LMM received                            : 20
      Invalid LMM received                          : 0
      LMR sent                                      : 20
      Valid LMR received                            : 10
      Invalid LMR received                          : 0
      Valid AIS frames transmitted                  : 0
      Valid AIS frames received                      : 0
      SLM sent                                      : 10
      Valid SLM received                            : 20
      Invalid SLM received                          : 0
      SLR sent                                      : 20
      Valid SLR received                            : 10
      Invalid SLR received                          : 0
    Remote MEP count: 2
      Identifier    MAC address        State    Interface
       2001     00:90:69:0b:7f:71       ok    ge-5/2/9.0
       4001     00:90:69:0b:09:c5       ok    ge-5/2/9.0
```

show oam ethernet connectivity-fault-management interfaces detail (One-Way ETH-DM)

`user@host` **show oam ethernet connectivity-fault-management interfaces detail**

```
Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up
  Maintenance domain name: md6, Format: string, Level: 6
    Maintenance association name: ma6, Format: string
    Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
     MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
```

```
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : no
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : no
    Statistics:
      CCMs sent                                     : 1590
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 1542035464

      1DMs sent                                     : 10
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0
    Remote MEP count: 1
      Identifier    MAC address        State    Interface
        201     00:90:69:0a:43:94       ok    ge-0/2/5.0
```

show oam ethernet connectivity-fault-management interfaces detail (Connection Protection TLV Configured)

`user@host`**show oam ethernet connectivity-fault-management interfaces detail**

```
Interface name: xe-6/2/0.0 , Interface status: Active, Link status: Up
  Maintenance domain name: md6, Format: string, Level: 6
 Maintenance association name: ma6, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: yes
```

```
  Prefer me: no, Protection in use: no, FRR Flag: no
MEP identifier: 1, Direction: down, MAC address: 00:19:e2:b1:14:30
MEP status: running
Defects:
  Remote MEP not receiving CCM                  : no
  Erroneous CCM received                        : no
  Cross-connect CCM received                    : no
  RDI sent by some MEP                          : no
  Some remote MEP's MAC in error state          : no
Statistics:
  CCMs sent                                     : 225
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 1244305646

  1DMs sent                                     : 0
  Valid 1DMs received                           : 0
  Invalid 1DMs received                         : 0
  Out of sync 1DMs received                     : 0
  DMMs sent                                     : 0
  Valid DMMs received                           : 0
  Invalid DMMs received                         : 0
  DMRs sent                                     : 0
  Valid DMRs received                           : 0
  Invalid DMRs received                         : 0
  LMMs sent                                     : 0
  Valid LMMs received                           : 0
  Invalid LMMs received                         : 0
  LMRs sent                                     : 0
  Valid LMRs received                           : 0
  Invalid LMRs received                         : 0
Remote MEP count: 1
  Identifier    MAC address        State    Interface
      2     00:90:69:7f:e4:30
```

show oam ethernet connectivity-fault-management interfaces

extensive

user@host> **show oam ethernet connectivity-fault-management interfaces extensive**

```
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Maintenance domain name: md0, Format: string, Level: 5
    Maintenance association name: ma1, Format: string
    Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: no
 MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : yes
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : yes

      Alarm Indication Signal                       : yes
    Statistics:
      CCMs sent                                     : 76
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 1645032434

      1DMs sent                                     : 0
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0

      Valid AIS frames transmitted                  : 0
      Valid AIS frames received                      : 0
      SLM sent                                      : 10
      Valid SLM received                            : 20
```

```
    Invalid SLM received                          : 0
    SLR sent                                      : 20
    Valid SLR received                            : 10
    Invalid SLR received                          : 0
  Remote MEP count: 2
    Identifier    MAC address        State    Interface
     2001     00:90:69:0b:7f:71       ok    ge-5/2/9.0
     4001     00:90:69:0b:09:c5       ok    ge-5/2/9.0
```

show oam ethernet connectivity-fault-management interfaces level

user@host> **show oam ethernet connectivity-fault-management interfaces level 7**

```
Interface       Link       Status           Level       MEP          Neighbors
                                                        Identifier
ge-3/0/0.0      Up         Active           7           201          0
xe-0/0/0.0      Up         Active           7           203          1
```

show oam ethernet connectivity-fault-management interfaces (trunk ports)

user@host> **show oam ethernet connectivity-fault-management interfaces**

```
Interface                  Link      Status       Level  MEP         Neighbors
                                                        Identifier
ge-4/0/1.0, vlan 100       Up        Active       5      100         0
ge-10/3/10.4091, vlan 4091 Down      Inactive     4      400         0
ge-4/0/0.0                 Up        Active       6      200         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-4/0/0.0**

```
Interface                  Link      Status       Level  MEP         Neighbors
                                                        Identifier
ge-4/0/0.0                 Up        Active       6      200         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-4/0/1.0 vlan 100**

```
Interface                   Link      Status       Level  MEP         Neighbors
                                                          Identifier
ge-4/0/1.0, vlan 100        Up        Active       5      100         0
```

user@host> **show oam ethernet connectivity-fault-management interfaces ge-10/3/10.4091 vlan 4091**

```
Interface                   Link      Status       Level  MEP         Neighbors
                                                          Identifier
ge-10/3/10.4091, vlan 4091  Down      Inactive     4      400         0
```

show oam ethernet connectivity-fault-management linktrace path-database

Syntax

show oam ethernet connectivity-fault-management linktrace path-database mac-address maintenance-association ***ma-name*** **maintenance-domain** ***md-name***

Release Information

Command introduced in Junos OS Release 9.0.

Description

On M320, MX Series, T320, and T640 routers, display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management maintenance linktrace database information.

Options

mac-address—Display connectivity fault management path database information for the specified MAC address of the remote host.

maintenance-association ***ma-name***—Display connectivity fault management path database information for the specified maintenance association.

maintenance-domain ***md-name***—Display connectivity fault management path database information for the specified maintenance domain.

Required Privilege Level

view

List of Sample Output

show oam ethernet connectivity-fault-management linktrace path-database on page 2742
show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands) on page 2743

Output Fields

Table 240 on page 2741 lists the output fields for the **show oam ethernet connectivity-fault-management linktrace path-database** command. Output fields are listed in the approximate order in which they appear.

Table 240: show oam ethernet connectivity-fault-management linktrace path-database Output Fields

Field Name	Field Description
Linktrace to	MAC address of the 802.1ag node to which the linktrace message is targeted.
Interface	Interface used by the local MEP to send the linktrace message (LTM).
Maintenance Domain	Maintenance domain identifier specified in the traceroute command.

Table 240: show oam ethernet connectivity-fault-management linktrace path-database Output Fields *(continued)*

Field Name	Field Description
Maintenance Association	Maintenance association identifier specified in the traceroute command.
Level	Maintenance domain level configured for the maintenance domain.
Local Mep	MEP identifier of the local MEP originating the linktrace.
Hop	Sequential hop count of the linktrace path.
TTL	Number of hops remaining in the linktrace message (LTM). The time to live (TTL) is decremented at each hop.
Source MAC address	MAC address of the 802.1ag node responding to the LTM or the source MAC address of the LTR.
Next hop MAC address	MAC address of the egress interface of the node to which the LTM is forwarded or the next-hop MAC address derived from the next egress identifier in the Egress-ID TLV of the LTR PDU.
Transaction Identifier	4-byte identifier maintained by the MEP. Each LTM uses a transaction identifier. The transaction identifier is maintained globally across all maintenance domains. Use the transaction identifier to match an incoming linktrace responses (LTR), with a previously sent LTM.

Sample Output

show oam ethernet connectivity-fault-management linktrace path-database

`user@host>` **show oam ethernet connectivity-fault-management linktrace path-database maintenance-domain MD1 maintenance-association MA1 00:01:02:03:04:05**

```
Linktrace to 00:01:02:03:04:05, Interface : ge-5/0/0.0
       Maintenance Domain: MD1, Level: 7
       Maintenance Association: MA1, Local Mep: 1

        Hop     TTL      Source MAC address        Next hop MAC address
```

```
      Transaction Identifier:100001
      1       63       00:00:aa:aa:aa:aa         00:00:ab:ab:ab:ab
      2       62       00:00:bb:bb:bb:bb         00:00:bc:bc:bc:bc
      3       61       00:00:cc:cc:cc:cc         00:00:cd:cd:cd:cd
      4       60       00:01:02:03:04:05         00:00:00:00:00:00
```

show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands)

`user@host>` **traceroute ethernet maintenance-domain md1 maintenance-association ma1 00:01:02:03:04:05**

```
Linktrace to 00:01:02:03:04:05, Interface : ge-5/0/0.0
      Maintenance Domain: MD1, Level: 7
      Maintenance Association: MA1, Local Mep: 1

      Hop     TTL      Source MAC address        Next hop MAC address
      Transaction Identifier:100002
      1       63       00:00:aa:aa:aa:aa         00:00:ab:ab:ab:ab
      2       62       00:00:bb:bb:bb:bb         00:00:bc:bc:bc:bc
      3       61       00:00:cc:cc:cc:cc         00:00:cd:cd:cd:cd
      4       60       00:01:02:03:04:05         00:00:00:00:00:00

      Transaction Identifier:100003
      1       63       00:00:aa:aa:aa:aa         00:00:ab:ab:ab:ab
      2       62       00:00:bb:bb:bb:bb         00:00:bc:bc:bc:bc
      3       61       00:00:cc:cc:cc:cc         00:00:cd:cd:cd:cd
      4       60       00:01:02:03:04:05         00:00:00:00:00:00
```

show oam ethernet connectivity-fault-management loss-statistics

Syntax

```
show oam ethernet connectivity-fault-management loss-statistics
maintenance-domain md-name
maintenance-association ma-name
<count entry-count>
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 11.1.

Description

On MX Series and ACX series routers with Ethernet interfaces, display ETH-LM statistics for on-demand mode only.

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

count *entry-count*—(Optional) Number of entries to display from the statistics table. The range of values is from 1 through 100. The default value is 100.

local-mep *local-mep-id*—(Optional) Numeric identifier of the local MEP. The range of values is from 1 through 8191.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. The range of values is from 1 through 8191.

Required Privilege Level

view

RELATED DOCUMENTATION

show oam ethernet connectivity-fault-management mep-statistics | 2764

Output Fields

Table 241 on page 2745 lists the output fields for the **show oam ethernet connectivity-fault-management loss-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 241: show oam ethernet connectivity-fault-management loss-statistics Output Fields

Output Field Name	Field Description
MEP identifier	Maintenance association end point (MEP) numeric identifier.
MAC address	Unicast MAC address configured for the MEP.
Remote MEP count	Number of remote MEPs (unless you specify the **remote-mep** option).
Remote MEP identifier	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Index	Index number that corresponds to the ETH-LM entry in the CFM database.
Near-end frame loss	Count of frame loss associated with ingress data frames.
Far-end frame loss	Count of frame loss associated with egress data frames.
Near-end loss ratio	Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the ingress interface.
Far-end loss ratio	Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the egress interface.
Average near-end frame loss	Average frame loss measured in this session associated with ingress data frames.
Average near-end loss ratio	Average frame loss ratio measured in this session associated with ingress data frames.
Average far-end frame loss	Average frame loss measured in this session associated with egress data frames.
Average far-end loss ratio	Average frame loss ratio measured in this session associated with egress data frames.
Near-end best case loss	Lowest frame loss measured in this session associated with ingress data frames.
Near-end best case loss ratio	Lowest frame loss ratio measured in this session associated with ingress data frames.

Table 241: show oam ethernet connectivity-fault-management loss-statistics Output Fields *(continued)*

Output Field Name	Field Description
Near-end worst case loss	Highest frame loss measured in this session associated with ingress data frames.
Near-end worst case loss ratio	Highest frame loss ratio measured in this session associated with ingress data frames.
Far-end best case frame loss	Lowest frame loss measured in this session associated with egress data frames.
Far-end best case loss ratio	Lowest frame loss ratio measured in this session associated with egress data frames.
Far-end worst case loss	Highest frame loss measured in this session associated with egress data frames.
Far-end worst case loss ratio	Highest frame loss ratio measured in this session associated with egress data frames.

show oam ethernet connectivity fault management loss statistics

`user@host>.` **show oam ethernet connectivity fault management loss statistics maintenance-domain md maintenance-association ma**

```
MEP identifier: 1, MAC address: 64:87:88:f9:7d:1b
Remote MEP count: 1

  Remote MAC address: 64:87:88:6a:da:94

    LM client session-id:4843
    CIR Loss measurement statistics:
    Index  Near-end      Far-end      Near-end       Far-end       Near-end
Far-end
           Frame loss    Total tx     Total rx       Frame loss    Total tx
Total rx
            (CIR)         (CIR)         (CIR)          (CIR)         (CIR)
 (CIR)
      1        0             245           245           0             244
    244
```

```
      2        0             488           488           0             489
    489
      3        0             732           732           0             733
    733
      4        0             977           977           0             976
    976
    EIR Loss measurement statistics:
    Index  Near-end      Far-end      Near-end       Far-end      Near-end
Far-end
           Frame loss    Total tx     Total rx       Frame loss    Total tx
Total rx
            (EIR)         (EIR)         (EIR)         (EIR)         (EIR)
(EIR)
      1        0             272           272           0             273
    273
      2        0             546           546           0             545
    545
      3        0             820           820           0             819
    819
      4        0             1092          1092          0             1093
    1093
    Total far-end Tx (CIR)             : 977
    Total near-end Rx (CIR)            : 977
    Total near-end loss(CIR)           : 0
    Total near-end loss ratio(CIR)     : 0.00000%
    Total near-end Tx (CIR)            : 976
    Total far-end Rx (CIR)             : 976
    Total far-end loss(CIR)            : 0
    Total far-end loss ratio(CIR)      : 0.00000%
    Average near-end loss(CIR)         : 0.00000
    Average near-end loss ratio(CIR)   : 0.00000%
    Average far-end loss(CIR)          : 0.00000
    Average far-end loss ratio(CIR)    : 0.00000%
    Near-end best case loss(CIR)       : 0
    Near-end best case loss ratio(CIR) : 0.00000%
    Near-end worst case loss(CIR)      : 0
    Near-end worst case loss ratio(CIR): 0.00000%
    Far-end best case loss(CIR)        : 0
    Far-end best case loss ratio(CIR)  : 0.00000%
    Far-end worst case loss(CIR)       : 0
    Far-end worst case loss ratio(CIR) : 0.00000%
    Total far-end Tx (EIR)             : 1092
    Total near-end Rx (EIR)            : 1092
    Total near-end loss(EIR)           : 0
```

```
Total near-end loss ratio(EIR)     : 0.00000%
Total near-end Tx (EIR)            : 1093
Total far-end Rx (EIR)             : 1093
Total far-end loss(EIR)            : 0
Total far-end loss ratio(EIR)      : 0.00000%
Average near-end loss(EIR)         : 0.00000
Average near-end loss ratio(EIR)   : 0.00000%
Average far-end loss(EIR)          : 0.00000
Average far-end loss ratio(EIR)    : 0.00000%
Near-end best case loss(EIR)       : 0
Near-end best case loss ratio(EIR) : 0.00000%
Near-end worst case loss(EIR)      : 0
Near-end worst case loss ratio(EIR): 0.00000%
Far-end best case loss(EIR)        : 0
Far-end best case loss ratio(EIR)  : 0.00000%
Far-end worst case loss(EIR)       : 0
Far-end worst case loss ratio(EIR) : 0.00000%
```

show oam ethernet connectivity-fault-management mep-database

Syntax

```
show oam ethernet connectivity-fault-management mep-database
maintenance-domain domain-name
maintenance-association ma-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
extensive
```

Release Information

Command introduced in Junos OS Release 8.4.
Support for ITU-T Y.1731 frame delay measurement added in Junos OS Release 9.5.
Support for ITU-T Y.1731 synthetic frame loss measurement added in Junos OS Release 13.2 for MX Series routers.
Support for ITU-T Y.1731 ethernet expected defect function (ETH-ED) added in Junos OS Release 19.1 for MX Series routers

> **NOTE:** Ethernet expected defect function (ETH-ED) will be supported on all MX series routers only when **enhanced-ip** mode is enabled. ETH-ED will not be supported if CFM is running in centralized mode.

Description

On M7i and M10i routers with Enhanced CFEB (CFEB-E), and on M320, M120, MX Series, ACX Series, T320, and T640 routers, display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

In addition, on M120, M320, and MX series routers, also display port status TLV, interface status TLV, and action profile information.

In addition, for Ethernet interfaces on MX Series routers , also display any ITU-T Y.1731 frame delay measurement (ETH-DM) frame counts.

For Ethernet interfaces on MX Series routers, display any ITU-T Y.1731 synthetic frame loss measurement (ETH-SLM) statistics and frame counts.

Options

maintenance-association *ma-name*—Name of the maintenance association.

maintenance-domain *domain-name*—Name of the maintenance domain.

local-mep-id—(Optional) Numeric identifier of local MEP.

remote-mep-id—(Optional) Numeric identifier of the remote MEP.

Required Privilege Level
view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2647
show oam ethernet connectivity-fault-management delay-statistics | 2679
show oam ethernet connectivity-fault-management interfaces | 2727
show oam ethernet connectivity-fault-management mep-statistics | 2764

List of Sample Output

show oam ethernet connectivity-fault-management mep-database on page 2756
show oam ethernet connectivity-fault-management mep-database (One-Way ETH-DM) on page 2757
show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 2757
show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event) on page 2758
show oam ethernet connectivity-fault-management mep-database (Connection Protection TLV Configured) on page 2758
show oam ethernet connectivity-fault-management mep-database on page 2760
show oam ethernet connectivity-fault-management mep-database (enhanced continuity measurement) on page 2761
show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 2762

Output Fields

Table 236 on page 2706 lists the output fields for the **show oam ethernet connectivity-fault-management mep-database** command. Output fields are listed in the approximate order in which they appear.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields

Field Name	Field Description
Maintenance domain name	Maintenance domain name.
Format (Maintenance domain)	Maintenance domain name format configured.
Level	Maintenance domain level configured.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
Maintenance association name	Maintenance association name.
Format (Maintenance association)	Maintenance association name format configured.
Continuity-check status	Continuity-check status.
Interval	Continuity-check message interval.
Loss-threshold	Lost continuity-check message threshold.
Connection Protection TLV	Status of the connection protection TLV, if configured on the MEP interface: **no**, **yes** If **yes**, then the transmitted connection protection TLV is decoded and the following three fields are displayed: **Prefer me**, **Protection in use**, **FRR Flag**
Prefer me	If set to **yes**, the path through which CCM was transmitted is preferred (unless the path fails). It is used for signaling a manual-switch command to remote side. Its value can be **yes** or **no**.
Protection in use	Used for protection decision coordination. Its value is set to **yes** if the endpoint transmitting the CCM is currently transmitting the user traffic to protection path. Its value can be **yes** or **no**.
FRR Flag	LSR/LER forwarding the CCM Frame into a bypass tunnel is set. Its value can be **yes** or **no**.
MEP identifier	Maintenance association end point (MEP) identifier.
Direction	MEP direction configured.
MAC address	MAC address configured for the MEP.
Auto-discovery	Whether automatic discovery is enabled or disabled.
Priority	Priority used for CCMs and linktrace messages transmitted by the MEP.
Interface name	Interface identifier.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
Interface status	Local interface status.
Link status	Local link status.
Remote MEP not receiving CCM	Whether the remote MEP is not receiving CCMs.
Erroneous CCM received	Whether erroneous CCMs have been received.
Cross-connect CCM received	Whether cross-connect CCMs have been received.
RDI sent by some MEP	Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.
CCMs sent	Number of CCMs transmitted.
CCMs received out of sequence	Number of CCMs received out of sequence.
LBMs sent	Number of loopback messages (LBMs) sent.
Valid in-order LBRs received	Number of loopback response messages (LBRs) received that were valid messages and in sequence.
1DMs sent	If the MEP is an initiator for a one-way ETH-DM session: Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.
Valid 1DMs received	If the MEP is a receiver for a one-way ETH-DM session: Number of valid 1DM frames received. For all other cases, this field displays **0**.
Invalid 1DMs received	If the MEP is a receiver for a one-way ETH-DM session: Number of invalid 1DM frames received. For all other cases, this field displays **0**.
Out of sync 1DMs received	If the MEP is a receiver for a one-way ETH-DM session: Number of out-of-sync one-way delay measurement request packets received.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
DMMs sent	If the MEP is an initiator for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays **0**.
Valid DMMs received	If the MEP is an initiator for a two-way ETH-DM session: Number of valid two-way delay measurement packets received.
Invalid DMMs received	If the MEP is an initiator for a two-way ETH-DM session: Number of invalid two-way delay measurement packets received.
DMRs sent	If the MEP is a responder for a ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays **0**.
Valid DMRs received	If the MEP is an initiator for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays **0**.
Invalid DMRs received	If the MEP is an initiator for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays **0**.
Valid out-of-order LBRs received	Number of LBRs received that were valid messages and not in sequence.
LBRs received with corrupted data	Number of LBRs received that were corrupted.
LBRs sent	Number of LBRs transmitted.
LTMs sent	Linktrace messages (LTMs) transmitted.
LTMs received	Linktrace messages received.
LTRs sent	Linktrace responses (LTRs) transmitted.
LTRs received	Linktrace responses received.
Sequence number of next LTM request	Sequence number of the next linktrace message request to be transmitted.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
LMM sent	If the interface is attached to an initiator MEP for a ETH-LM session: Number of loss measurement message (LMM) PDU frames sent to the peer MEP in this session.
Valid LMM received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of valid loss measurement request packets received.
Invalid LMM received	If the interface is attached to an initiator MEP for a ETH LM session: Number of invalid loss measurement request packets received.
LMR sent	If the interface is attached to a responder MEP for a ETH-LM session: Number of loss measurement reply (LMR) frames sent.
Valid LMR received	If the interface is attached to an initiator MEP for a ETH LM session: Number of valid LMR frames received.
Invalid LMR received	If the interface is attached to an initiator MEP for a ETH-LM session: Number of invalid LMR frames received.
SLM sent	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of synthetic loss measurement (SLM) request packets transmitted from the source MEP to the remote or destination MEP in this session.
Valid SLM received	If the interface is attached to a responder MEP for a ETH-SLM session: Number of valid SLM PDUs transmitted from the source MEP to the remote or destination MEP.
Invalid SLM received	If the interface is attached to a responder MEP for a ETH-SLM session: Number of invalid SLM PDUs transmitted from the source MEP to the remote or destination MEP.
SLR sent	If the interface is attached to a responder MEP for a ETH-SLM session: Number detail extensive of synthetic loss reply (SLR) frames sent.
Valid SLR received	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of valid SLR PDUs that the source MEP received from the remote or destination MEP.
Invalid SLR received	If the interface is attached to an initiator MEP for a ETH-SLM session: Number of invalid SLR PDUs that the source MEP received from the remote or destination MEP.
Remote MEP identifier	MEP identifier of the remote MEP.
State (remote MEP)	State of the remote MEP: **idle**, **start**, **ok**, or **failed**.

Table 242: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

Field Name	Field Description
MAC address	MAC address of the remote MEP.
Type	Whether the remote MEP MAC address was learned using automatic discovery or configured.
Interface	Interface of the remote MEP. A seven-digit number is appended if CFM is configured to run on a routing instance of type VPLS.
Last flapped	Date, time, and how long ago the remote MEP interface went from down to up. The format is **Last flapped: *year-month-day hours:minutes:seconds timezone* (*hours:minutes:seconds* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.
Remote defect indication	Whether the remote defect indication (RDI) bit is set in messages that have been received or transmitted.
Port status TLV	• In the Maintenance domain section, displays the last transmitted port status TLV value. • In the Remote MEP section, displays the last value of port status TLV received from the remote MEP. In the Action profile section, displays, the last occurred event **port-status-tlv blocked** event. This event occurred due to the reception of **blocked** value in the port status TLV from remote MEP.
Interface status TLV	• In the Maintenance domain section, displays the last transmitted interface status TLV value. • In the Remote MEP section, displays the last value of interface status TLV received from the remote MEP. In the Action profile section, if displays, the last occurred event interface-status-tlv event (either **lower-layer-down** or **down**). This event occurred due to the reception of either lower or **down** value in the interface status TLV from remote MEP.
Action profile	Name of the action profile occurrence associated with a remote MEP.
Last event	When an action profile occurs, displays the last event that triggered it.
Last event cleared	When all the configured and occurred events (under action profile) are cleared, then the action taken gets reverted (such as down interface is made up) and the corresponding time is noted and displayed.
Action	Action taken and the corresponding time of the action occurrence.

Sample Output

show oam ethernet connectivity-fault-management mep-database

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200**

```
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
  Maintenance association name: vpls-vlan200, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
  Auto-discovery: enabled, Priority: 0
 Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: no  Interface name: ge-0/0/1.0, Interface status:
Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                  : no
    Erroneous CCM received                        : no
    Cross-connect CCM received                    : no
    RDI sent by some MEP                          : no
  Statistics:
    CCMs sent                                     : 1476
    CCMs received out of sequence                 : 0
    LBMs sent                                     : 85
    Valid in-order LBRs received                  : 78
    Valid out-of-order LBRs received              : 0
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 1
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 1
    Sequence number of next LTM request           : 1
    1DMs sent                                     : 0
    Valid 1DMs received                           : 0
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      100     00:19:e2:b2:81:4b       ok  vt-0/1/10.1049088
```

show oam ethernet connectivity-fault-management mep-database (One-Way ETH-DM)

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6 maintenance-domain ma6**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                  : no
    Erroneous CCM received                        : no
    Cross-connect CCM received                    : no
    RDI sent by some MEP                          : no
  Statistics:
    CCMs sent                                     : 1590
    CCMs received out of sequence                 : 0
    LBMs sent                                     : 0
    Valid in-order LBRs received                  : 0
    Valid out-of-order LBRs received              : 0
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 0
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 0
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 10
    Valid 1DMs received                           : 0
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      201     00:90:69:0a:43:94       ok    ge-0/2/5.0
```

show oam ethernet connectivity-fault-management mep-database local-mep remote-mep

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200 local-mep 200 remote-mep 100**

```
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
  Maintenance association name: vpls-vlan200, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 100, State: ok
    MAC address: 00:19:e2:b2:81:4b, Type: Learned
    Interface: vt-0/1/10.1049088
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
```

show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event)

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5 remote-mep 200**

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 200, State: ok
    MAC address: 00:05:85:73:96:1f, Type: Configured
    Interface: ge-1/0/8.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: lower-layer-down
    Action profile: juniper
      Last event: Interface-status-tlv lower-layer-down
      Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
```

show oam ethernet connectivity-fault-management mep-database

(Connection Protection TLV Configured)

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5**

If connection-protection is not enabled on down MEPs, but connection-protection TLV is used, MX always sets the protection-in-use flag in connection-protection tlv, while CCMs are sent out. During reversion, this is an indicator to the receiver that protect-path is in use, otherwise the peer (receiver) assumes working is active and reversion does not work as expected. Setting this bit does not affect protection-switching/traffic-loss.

```
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 1, Direction: down, MAC address: 00:19:e2:b1:14:30
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: yes
    Prefer me: no, Protection in use: no, FRR Flag: no
  Interface name: xe-6/2/0.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                 : no
    Erroneous CCM received                       : no
    Cross-connect CCM received                   : no
    RDI sent by some MEP                         : no
    Some remote MEP's MAC in error state         : no
  Statistics:
    CCMs sent                                    : 251
    CCMs received out of sequence                : 0
    LBMs sent                                    : 0
    Valid in-order LBRs received                 : 0
    Valid out-of-order LBRs received             : 0
    LBRs received with corrupted data            : 0
    LBRs sent                                    : 0
    LTMs sent                                    : 0
    LTMs received                                : 0
    LTRs sent                                    : 0
    LTRs received                                : 0
    Sequence number of next LTM request          : 0
    1DMs sent                                    : 0
    Valid 1DMs received                          : 0
    Invalid 1DMs received                        : 0
    Out of sync 1DMs received                    : 0
    DMMs sent                                    : 0
    Valid DMMs received                          : 0
```

```
    Invalid DMMs received                        : 0
    DMRs sent                                    : 0
    Valid DMRs received                          : 0
    Invalid DMRs received                        : 0
    LMMs sent                                    : 0
    Valid LMMs received                          : 0
    Invalid LMMs received                        : 0
    LMRs sent                                    : 0
    Valid LMRs received                          : 0
    Invalid LMRs received                        : 0
  Remote MEP count: 1
   Identifier    MAC address        State    Interface
        2     00:90:69:7f:e4:30
```

show oam ethernet connectivity-fault-management mep-database

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5**

```
Maintenance association name: ma1, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
MEP identifier: 1, Direction: down, MAC address: 00:14:f6:b6:01:fe
Auto-discovery: enabled, Priority: 0
Interface name: ge-1/0/0.0, Interface status: Active, Link status: Up

Defects:
Remote MEP not receiving CCM         : no
Erroneous CCM received               : no
Cross-connect CCM received           : no
RDI sent by some MEP                 : no

Statistics:
CCMs sent                            : 328703
CCMs received out of sequence        : 0
LBMs sent                            : 85
Valid in-order LBRs received         : 78
Valid out-of-order LBRs received     : 0
LBRs received with corrupted data    : 0
LBRs sent                            : 0
LTMs sent                            : 0
LTMs received                        : 0
LTRs sent                            : 0
LTRs received                        : 0
```

```
Sequence number of next LTM request  : 0
1DMs sent                            : 10
Valid 1DMs received                  : 10
Invalid 1DMs received                : 0
DMMs sent                            : 20
DMRs sent                            : 0
Valid DMRs received                  : 10
Invalid DMRs received                : 0
LMM sent                             : 10
Valid LMM received                   : 20
Invalid LMM received                 : 0
LMR sent                             : 20
Valid LMR received                   : 10
Invalid LMR received                 : 0
SLM sent                                    : 10
Valid SLM received                          : 20
Invalid SLM received                        : 0
SLR sent                                    : 20
Valid SLR received                          : 10
Invalid SLR received                        : 0

Remote MEP count                     : 1

Identifier     MAC address         State     Interface
    2       00:12:1e:fb:ea:7d       ok        ge-1/0/0.0
```

show oam ethernet connectivity-fault-management mep-database (enhanced continuity measurement)

user@host> **show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001**

```
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up
Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

Remote MEP identifier: 1001, State: ok
MAC address  : 00:19:e2:b0:74:00, Type: Learned
Interface    : ge-2/0/0.0
Last flapped  : Never
```

```
+ Continuity  : 91%, Admin-enable duration: 2100sec, Oper-down duration: 100sec
Remote defect indication: false
Port status TLV: none
Interface status TLV: none
```

show oam ethernet connectivity-fault-management mep-database local-mep remote-mep

When the timer is not running:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6 maintenance-association ma6 local-mep 201 remote-mep 101 extensive**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: up, MAC address: 00:24:dc:48:46:cd
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: no
  Chassis ID: 00:24:dc:48:47:f2
  Management Address: 10.216.34.30
  Sendid TLV: no
  Interface name: ge-5/1/9.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 101, State: ok
    MAC address: 00:22:83:db:4c:5b, Type: Configured
    Interface: ge-5/3/0.0
    Last flapped: 2019-02-05 00:45:57 PST (00:54:51 ago)
    Continuity: 99%, Admin-enable duration: 3367sec, Oper-down duration: 43sec
    Effective loss threshold: 3 frames
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
    Remote Management Address: 0.0.0.0
    Sendid TLV: no
    Sender ID Remote Chassis Subtype: 0
    EDM time remaining: N/A
```

When the timer is running:

`user@host>` **show oam ethernet connectivity-fault-management mep-database maintenance-domain md6 maintenance-association ma6 local-mep 201 remote-mep 101 extensive**

```
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: up, MAC address: 00:24:dc:48:46:cd
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: no
  Chassis ID: 00:24:dc:48:47:f2
  Management Address: 10.216.34.30
  Sendid TLV: no
  Interface name: ge-5/1/9.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 101, State: ok
    MAC address: 00:22:83:db:4c:5b, Type: Configured
    Interface: ge-5/3/0.0
    Last flapped: 2019-02-05 00:45:57 PST (00:56:16 ago)
    Continuity: 99%, Admin-enable duration: 3451sec, Oper-down duration: 43sec
    Effective loss threshold: 3 frames
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
    Remote Management Address: 0.0.0.0
    Sendid TLV: no
    Sender ID Remote Chassis Subtype: 0
    EDM time remaining: 894 secs
```

show oam ethernet connectivity-fault-management mep-statistics

Syntax

```
show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain md-name
maintenance-association ma-name
<mep mep-id>
<remote-mep remote-mep-id>
<count entry-count>
```

Release Information

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 11.4 for EX Series switches.
Support for ITU-T Y.1731 Ethernet synthetic frame loss measurement (ETH-SLM) added in Junos OS Release 13.2 for MX Series routers.

Description

On MX Series and ACX Series routers and EX Series switches with Ethernet interfaces, display ETH-DM statistics and ETH-DM frame counts.

For Ethernet interfaces on MX Series routers, display any ITU-T Y.1731 synthetic frame loss measurement (ETH-SLM) statistics and frame counts.

Options

maintenance-domain *md-name*—Name of an existing CFM maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

mep *mep-id*—(Optional) Numeric identifier of the local MEP. The range of values is 1 through 8192. On EX Series switches, the range of values is 1 through 8191.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. The range of values is 1 through 8192. On EX Series switches, the range of values is 1 through 8191.

count *entry-count*—(Optional) Number of entries to display from the statistics table. The range of values is 1 through 100. The default value is 100 entries.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management statistics | 2647

show oam ethernet connectivity-fault-management delay-statistics | 2679
show oam ethernet connectivity-fault-management interfaces | 2727
show oam ethernet connectivity-fault-management mep-database | 2749

List of Sample Output

show oam ethernet connectivity-fault-management mep-statistics (CIR counters only) on page 2767
show oam ethernet connectivity-fault-management mep-statistics (CIR and EIR counters enabled) on page 2769
show oam ethernet connectivity-fault-management mep-statistics remote-mep (CIR counters only) on page 2771
show oam ethernet connectivity-fault-management mep-statistics remote-mep (CIR and EIR counters enabled) on page 2773
show oam ethernet connectivity-fault-management mep-statistics on page 2775
show oam ethernet connectivity-fault-management mep-statistics remote-mep on page 2776
show oam ethernet connectivity-fault-management mep-statistics local-mep remote-mep on page 2778

Output Fields

Table 243 on page 2765 lists the output fields for the **show oam ethernet connectivity-fault-management mep-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 243: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields

Output Field Name	Field Description
MEP identifier	Maintenance association end point (MEP) numeric identifier.
MAC address	Unicast MAC address configured for the MEP.
Remote MEP count	Number of remote MEPs (unless you specify the **remote-mep** option).
CCMs sent	Number of continuity check messages (CCMs) sent.
CCMs received	Number of continuity check messages (CCMs) received for a specific remote MEP and maintenance association.
CCMs received out of sequence	Number of continuity check messages (CCMs) received that were not in sequence.
Remote MEP identifier	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Index	Index number that corresponds to the ETH-DM entry in the CFM database.

Table 243: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields *(continued)*

Output Field Name	Field Description
One-way delay (usec)	For a one-way ETH-DM session, the frame delay time, in microseconds, measured at the receiver MEP. For a detailed description of one-way Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.
Two-way delay (usec)	For a two-way ETH-DM session, the frame delay time, in microseconds, measured at the initiator MEP. For a detailed description of two-way Ethernet frame delay measurement, see the *ITU-T Y.1731 Ethernet Service OAM* topics in the *Junos OS Network Interfaces Library for Routing Devices*.
Average one-way delay	Average one-way frame delay for the statistics displayed.
Average one-way delay variation	Average one-way “frame jitter” for the statistics displayed.
Best-case one-way delay	Lowest one-way frame delay for the statistics displayed.
Worst-case one-way delay	Highest one-way frame delay for the statistics displayed.
Average two-way delay	Average two-way frame delay for the statistics displayed.
Average two-way delay variation	Average two-way “frame jitter” for the statistics displayed.
Best-case two-way delay	Lowest two-way frame delay for the statistics displayed.
Worst-case two-way delay	Highest two-way frame delay calculated in this session.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLM packets received	Total number of synthetic loss message (SLM) PDU frames that the remote MEP received from the source MEP during this ETH-SLM session.
SLR packets sent	Total number of synthetic loss reply (SLR) PDU frames that the remote MEP sent to the source MEP during this measurement session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames that the source MEP received from the remote MEP during this measurement session.

Table 243: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields *(continued)*

Output Field Name	Field Description
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

show oam ethernet connectivity-fault-management mep-statistics (CIR counters only)

`user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma-1 local-mep 3 remote-mep 103 count 3**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count                    : 1
CCMs sent                           : 6550
CCMs received out of sequence       : 0
LBMs sent                           : 0
Valid in-order LBRs received        : 0
Valid out-of-order LBRs received    : 0
LBRs received with corrupted data   : 0
LBRs sent                           : 0
LTMs sent                           : 0
```

```
LTMs received                       : 0
LTRs sent                           : 0
LTRs received                       : 0
Sequence number of next LTM request : 0
1DMs sent                           : 5
Valid 1DMs received                 : 0
Invalid 1DMs received               : 0
DMMs sent                           : 5
DMRs sent                           : 0
Valid DMRs received                 : 5
Invalid DMRs received               : 0
LMM sent                            : 5
Valid LMM received                  : 5
Invalid LMM received                : 0
LMR sent                            : 0
Valid LMR received                  : 5
Invalid LMR received                : 0
Remote MEP identifier               : 101
Remote MAC address                  : 00:05:85:73:39:4a

Delay measurement statistics:
Index       One-way delay         Two-way delay
               (usec)                (usec)
  1             259                   519
  2             273                   550
  3             287                   571
  4             299                   610
  5             313                   650

Average one-way delay                 : 286 usec
Average one-way delay variation       : 62 usec
Best case one-way delay               : 259 usec
Average two-way delay                 : 580 usec
Average two-way delay variation       : 26 usec
Best case two-way delay               : 519 usec
Worst case two-way delay              : 650 usec

Loss measurement statistics:
Index     Near-end     Far-end       Near-end     Far-end
          Frame loss   Frame loss    Frame loss   Frame loss
            (CIR)       (CIR)          (EIR)        (EIR)
  1           9           9
  2           3           5
  3           7           5
```

```
  4           9           6
  5           3           6

Average near-end loss (CIR)            : 6.2
Average near-end loss ratio (CIR)      : 6.2%
Average far-end loss (CIR)             : 6.2
Average far-end loss ratio (CIR)       : 6.2%
Near-end best case loss (CIR)          : 3
Near-end best case loss ratio (CIR)    : 3%
Near-end worst case loss (CIR)         : 9
Near-end worst case loss ratio (CIR)   : 9%
Far-end best case loss (CIR)           : 5
Far-end best case loss ratio (CIR)     : 5%
Far-end worst case loss (CIR)          : 9
Far-end worst case loss ratio (CIR)    : 9%
```

show oam ethernet connectivity-fault-management mep-statistics (CIR and EIR counters enabled)

user@host> **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma-1 local-mep 3 remote-mep 103 count 3**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count                     : 1
CCMs sent                            : 6550
CCMs received out of sequence        : 0
LBMs sent                            : 0
Valid in-order LBRs received         : 0
Valid out-of-order LBRs received     : 0
LBRs received with corrupted data    : 0
LBRs sent                            : 0
LTMs sent                            : 0
LTMs received                        : 0
LTRs sent                            : 0
LTRs received                        : 0
Sequence number of next LTM request  : 0
1DMs sent                            : 5
Valid 1DMs received                  : 0
Invalid 1DMs received                : 0
DMMs sent                            : 5
DMRs sent                            : 0
Valid DMRs received                  : 5
Invalid DMRs received                : 0
LMM sent                             : 5
```

```
alid LMM received                    : 5
Invalid LMM received                 : 0
LMR sent                             : 0
Valid LMR received                   : 5
Invalid LMR received                 : 0
Remote MEP identifier                : 101
Remote MAC address                   : 00:05:85:73:39:4a

Delay measurement statistics:
Index       One-way delay         Two-way delay
              (usec)                (usec)
  1            259                   519
  2            273                  550
  3            287                  571
  4            299                  610
  5            313                  650

Average one-way delay                  : 286 usec
Average one-way delay variation        : 62 usec
Best case one-way delay                : 259 usec
Average two-way delay                  : 580 usec
Average two-way delay variation        : 26 usec
Best case two-way delay                : 519 usec
Worst case two-way delay               : 650 usec

Loss measurement statistics:
Index     Near-end     Far-end       Near-end     Far-end
          Frame loss   Frame loss    Frame loss   Frame loss
           (CIR)         (CIR)        (EIR)         (EIR)
  1          9             9            2            4
  2          3             5            4            6
  3          7             5            0            2
  4          9             6            8            2
  5          3             6            6            4

Average near-end loss (CIR)              : 6.2
Average near-end loss ratio (CIR)        : 6.2%
Average far-end loss (CIR)               : 6.2
Average far-end loss ratio (CIR)         : 6.2%
Near-end best case loss (CIR)            : 3
Near-end best case loss ratio (CIR)      : 3%
Near-end worst case loss (CIR)           : 9
Near-end worst case loss ratio (CIR)     : 9%
Far-end best case loss (CIR)             : 5
```

```
Far-end best case loss ratio (CIR)        : 5%
Far-end worst case loss (CIR)             : 9
Far-end worst case loss ratio (CIR)       : 9%
Average near-end loss (EIR)               : 4
Average near-end loss ratio (EIR)         : 4%
Average far-end loss (EIR)                : 3.4
Average far-end loss ratio (EIR)          : 3.4%
Near-end best case loss (EIR)             : 0
Near-end best case loss ratio (EIR)       : 0%
Near-end worst case loss (EIR)            : 8
Near-end worst case loss ratio (EIR)      : 8%
Far-end best case loss (EIR)              : 2
Far-end best case loss ratio (EIR)        : 2%
Far-end worst case loss (EIR)             : 6
Far-end worst case loss ratio (EIR)       : 6%
```

show oam ethernet connectivity-fault-management mep-statistics remote-mep (CIR counters only)

`user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma-1 local-mep 3 remote-mep 103 count 3 remote-mep 101**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
CCMs sent                              : 7762
CCMs received out of sequence          : 0
LBMs sent                              : 0
Valid in-order LBRs received           : 0
Valid out-of-order LBRs received       : 0
LBRs received with corrupted data      : 0
LBRs sent                              : 0
LTMs sent                              : 0
LTMs received                          : 0
LTRs sent                              : 0
LTRs received                          : 0
Sequence number of next LTM request    : 0
1DMs sent                              : 5
Valid 1DMs received                    : 0
Invalid 1DMs received                  : 0
DMMs sent                              : 5
DMRs sent                              : 0
Valid DMRs received                    : 5
Invalid DMRs received                  : 0
LMM sent                               : 5
Valid LMM received                     : 5
```

```
Invalid LMM received                  : 0
LMR sent                              : 0
Valid LMR received                    : 5
Invalid LMR received                  : 0
Remote MEP identifier                 : 101
Remote MAC address                    : 00:05:85:73:39:4a

Delay measurement statistics:
Index       One-way delay         Two-way delay
               (usec)                (usec)
  1             259                   519
  2             273                   550
  3             287                   571
  4             299                   610
  5             313                   650

Average one-way delay                  : 286 usec
Average one-way delay variation        : 62 usec
Best case one-way delay                : 259 usec
Average two-way delay                  : 580 usec
Average two-way delay variation        : 26 usec
Best case two-way delay                : 519 usec
Worst case two-way delay               : 650 usec

Loss measurement statistics:
Index     Near-end     Far-end       Near-end     Far-end
          Frame loss   Frame loss    Frame loss   Frame loss
            (CIR)        (CIR)         (EIR)       (EIR)
  1           9            9
  2           3            5
  3           7            5
  4           9            6
  5           3            6
Average near-end loss (CIR)              : 6.2
Average near-end loss ratio (CIR)        : 6.2%
Average far-end loss (CIR)               : 6.2
Average far-end loss ratio (CIR)         : 6.2%
Near-end best case loss (CIR)            : 3
Near-end best case loss ratio (CIR)      : 3%
Near-end worst case loss (CIR)           : 9
Near-end worst case loss ratio (CIR)     : 9%
Far-end best case loss (CIR)             : 5
Far-end best case loss ratio (CIR)       : 5%
Far-end worst case loss (CIR)            : 9
```

```
Far-end worst case loss ratio (CIR)       : 9%
Average near-end loss (EIR)               : 4
Average near-end loss ratio (EIR)         : 4%
Average far-end loss (EIR)                : 3.4
Average far-end loss ratio (EIR)          : 3.4%
Near-end best case loss (EIR)             : 0
Near-end best case loss ratio (EIR)       : 0%
Near-end worst case loss (EIR)            : 8
Near-end worst case loss ratio (EIR)      : 8%
Far-end best case loss (EIR)              : 2
Far-end best case loss ratio (EIR)        : 2%
Far-end worst case loss (EIR)             : 6
Far-end worst case loss ratio (EIR)       : 6%
```

show oam ethernet connectivity-fault-management mep-statistics remote-mep (CIR and EIR counters enabled)

`user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma-1 local-mep 3 remote-mep 103 count 3 remote-mep 101**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
CCMs sent                            :7762
CCMs received out of sequence        : 0
LBMs sent                            : 0
Valid in-order LBRs received         : 0
Valid out-of-order LBRs received     : 0
LBRs received with corrupted data    : 0
LBRs sent                            : 0
LTMs sent                            : 0
LTMs received                        : 0
LTRs sent                            : 0
LTRs received                        : 0
Sequence number of next LTM request  : 0
1DMs sent                            : 5
Valid 1DMs received                  : 0
Invalid 1DMs received                : 0
DMMs sent                            : 5
DMRs sent                            : 0
Valid DMRs received                  : 5
Invalid DMRs received                : 0
LMM sent                             : 5
Valid LMM received                   : 5
Invalid LMM received                 : 0
LMR sent                             : 0
```

```
Valid LMR received                    : 5
Invalid LMR received                  : 0
Remote MEP identifier                 : 101
Remote MAC address                    : 00:05:85:73:39:4a

Delay measurement statistics:
Index       One-way delay         Two-way delay
               (usec)                (usec)
  1             259                   519
  2             273                   550
  3             287                   571
  4             299                   610
  5             313                   650

Average one-way delay                 : 286 usec
Average one-way delay variation       : 62 usec
Best case one-way delay               : 259 usec
Average two-way delay                 : 580 usec
Average two-way delay variation       : 26 usec
Best case two-way delay               : 519 usec
Worst case two-way delay              : 650 usec

Loss measurement statistics:
Index     Near-end     Far-end       Near-end     Far-end
          Frame loss   Frame loss    Frame loss   Frame loss
            (CIR)       (CIR)          (EIR)        (EIR)
  1          10           8              5           12
  2          12           7              6           16
  3          7            5              0           2
  4          9            6              8           2
  5          3            6              6           4

Average near-end loss (CIR)             : 6.2
Average near-end loss ratio (CIR)       : 6.2%
Average far-end loss (CIR)              : 6.2
Average far-end loss ratio (CIR)        : 6.2%
Near-end best case loss (CIR)           : 3
Near-end best case loss ratio (CIR)     : 3%
Near-end worst case loss (CIR)          : 9
Near-end worst case loss ratio (CIR)    : 9%
Far-end best case loss (CIR)            : 5
Far-end best case loss ratio (CIR)      : 5%
Far-end worst case loss (CIR)           : 9
Far-end worst case loss ratio (CIR)     : 9%
```

```
Average near-end loss (EIR)             : 4
Average near-end loss ratio (EIR)       : 4%
Average far-end loss (EIR)              : 3.4
Average far-end loss ratio (EIR)        : 3.4%
Near-end best case loss (EIR)           : 0
Near-end best case loss ratio (EIR)     : 0%
Near-end worst case loss (EIR)          : 8
Near-end worst case loss ratio (EIR)    : 8%
Far-end best case loss (EIR)            : 2
Far-end best case loss ratio (EIR)      : 2%
Far-end worst case loss (EIR)           : 6
Far-end worst case loss ratio (EIR)     : 6%
```

show oam ethernet connectivity-fault-management mep-statistics

user@host> **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma-1**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count: 1
  CCMs sent                                     : 6550
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 0
  1DMs sent                                     : 5
  Valid 1DMs received                           : 0
  Invalid 1DMs received                         : 0
  DMMs sent                                     : 5
  DMRs sent                                     : 0
  Valid DMRs received                           : 5
  Invalid DMRs received                         : 0
  SLM sent                                      : 10
  Valid SLM received                            : 20
  Invalid SLM received                          : 0
  SLR sent                                      : 20
```

```
  Valid SLR received                              : 10
  Invalid SLR received                            : 0

  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        259            519
      2        273            550
      3        287            571
      4        299            610
      5        313            650
    Average one-way delay          : 286 usec
    Average one-way delay variation: 62 usec
    Best case one-way delay        : 259 usec
    Worst case one-way delay       : 313 usec
    Average two-way delay          : 580 usec
    Average two-way delay variation: 26 usec
    Best case two-way delay        : 519 usec
    Worst case two-way delay       : 650 usec    Synthetic Loss measurement
statistics:
     SLM packets sent                             : 100
     SLM packets received                         : 0
     SLR packets sent                             : 100
     SLR packets received                         : 0
     Accumulated SLM statistics:
     Local TXFC1 value                            : 100
     Local RXFC1 value                            : 100
     Last Received SLR frame TXFCftc              : 100
     Last Received SLR frame TXFCbtc              : 100
     SLM Frame Loss:
     Frame Loss (far-end)                         : 0 (0.00 %)
     Frame Loss (near-end)                        : 0 (0.00 %)
```

show oam ethernet connectivity-fault-management mep-statistics remote-mep

`user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma1 remote-mep 101**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
  CCMs sent                                       : 7762
  CCMs received out of sequence                   : 0
```

```
  LBMs sent                                        : 0
  Valid in-order LBRs received                     : 0
  Valid out-of-order LBRs received                 : 0
  LBRs received with corrupted data                : 0
  LBRs sent                                        : 0
  LTMs sent                                        : 0
  LTMs received                                    : 0
  LTRs sent                                        : 0
  LTRs received                                    : 0
  Sequence number of next LTM request              : 0
  1DMs sent                                        : 5
  Valid 1DMs received                              : 0
  Invalid 1DMs received                            : 0
  DMMs sent                                        : 5
  DMRs sent                                        : 0
  Valid DMRs received                              : 5
  Invalid DMRs received                            : 0
  SLM sent                                         : 10
  Valid SLM received                               : 20
  Invalid SLM received                             : 0
  SLR sent                                         : 20
  Valid SLR received                               : 10
  Invalid SLR received                             : 0

  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        259            519
      2        273            550
      3        287            571
      4        299            610
      5        313            650
    Average one-way delay          : 286 usec
    Average one-way delay variation: 62 usec
    Best case one-way delay        : 259 usec
    Worst case one-way delay       : 313 usec
    Average two-way delay          : 580 usec
    Average two-way delay variation: 26 usec
    Best case two-way delay        : 519 usec
    Worst case two-way delay       : 650 usec    Synthetic Loss measurement
statistics:
     SLM packets sent                             : 100
```

```
    SLM packets received                        : 0
    SLR packets sent                            : 100
    SLR packets received                        : 0
    Accumulated SLM statistics:
    Local TXFC1 value                           : 100
    Local RXFC1 value                           : 100
    Last Received SLR frame TXFCftc             : 100
    Last Received SLR frame TXFCbtc             : 100
    SLM Frame Loss:
    Frame Loss (far-end)                        : 0 (0.00 %)
    Frame Loss (near-end)                       : 0 (0.00 %)
```

show oam ethernet connectivity-fault-management mep-statistics local-mep remote-mep

`user@host>` **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md1 maintenance-association ma1 local-mep 121 remote-mep 101**

```
MEP identifier: 1, MAC address: 3c:61:04:25:fa:95
Remote MEP count: 1
  CCMs sent                                     : 875
  CCMs Received                                 : 300
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           :  12
  1DMs sent                                     : 0
  Valid 1DMs received                           : 0
  Invalid 1DMs received                         : 0
  Out of sync 1DMs received                     : 0
  DMMs sent                                     : 0
  Valid DMMs received                           : 0
  Invalid DMMs received                         : 0
  DMRs sent                                     : 0
  Valid DMRs received                           : 0
  Invalid DMRs received                         : 0
  LMMs sent                                     : 0
```

```
Valid LMMs received                          : 0
Invalid LMMs received                        : 0
LMRs sent                                    : 0
Valid LMRs received                          : 0
Invalid LMRs received                        : 0
SLMs sent                                    : 0
Valid SLMs received                          : 0
Invalid SLMs received                        : 0
SLRs sent                                    : 0
Valid SLRs received                          : 0
Invalid SLRs received                        : 0
Valid AISs generated                         : 0
Valid AISs received                          : 0
```

show oam ethernet connectivity-fault-management path-database

Syntax

```
show oam ethernet connectivity-fault-management path-database
<host-mac-address>
<maintenance-association ma-name>
<maintenance-domain domain-name>
```

Release Information

Command introduced in Junos OS Release 8.4.

Description

On M7i and M10i with Enhanced CFEB (CFEB-E), M320, MX Series, ACX Series, T320, and T640 routers, display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management path database information for a host configured with an MEP.

Options

host-mac-address—(Optional) Display connectivity fault management path database information for a specified Ethernet host.

maintenance-association *ma-name*—(Optional) Display connectivity fault management path database information for the specified maintenance association.

maintenance-domain *domain-name*—(Optional) Display connectivity fault management path database information for the specified maintenance domain.

Required Privilege Level

view

List of Sample Output

show oam ethernet connectivity-fault-management path-database on page 2781

Output Fields

Table 244 on page 2780 lists the output fields for the **show oam ethernet connectivity-fault-management path-database** command. Output fields are listed in the approximate order in which they appear.

Table 244: show oam ethernet connectivity-fault-management path-database Output Fields

Field Name	Field Description
Linktrace to	MAC address of the remote MEPs in the path.
Interface	Interface identifier.

Table 244: show oam ethernet connectivity-fault-management path-database Output Fields *(continued)*

Field Name	Field Description
Maintenance domain name	Maintenance domain name.
Format (Maintenance domain)	Maintenance domain name format configured.
Level	Maintenance domain level configured.
Maintenance association name	Maintenance association name.
Local Mep	Local MEP identifier.

Sample Output

show oam ethernet connectivity-fault -management path-database

`user@host>` **show oam ethernet connectivity–fault-management path-database maintenance-domain md1 maintenance-association ma1 00:05:85:79:39:ef**

```
Linktrace to 00:05:85:79:39:ef, Interface : ge-3/0/0
      Maintenance Domain: md1, Level: 7
      Maintenance Association: ma1, Local Mep: 201
```

show oam ethernet connectivity-fault-management policer

Syntax

```
show oam ethernet connectivity-fault-management policer <maintenance-domain md-name>
  <maintenance-association ma-name>
```

Release Information

Command introduced in Junos OS Release 10.0.

Description

On M120, M320, MX Series, T320, and T640 routers displays connectivity-fault-management policer statistics.

Options

This command has the following options:

maintenance-domain *md-name*—Name of an existing CFM maintenance domain. If this option is not specified, policer statistics are displayed for all maintenance associations for all maintenance domains.

maintenance-association *ma-name*—Name of an existing CFM maintenance association. If this option is not specified, policer statistics are displayed for all maintenance associations for given maintenance domain. This option cannot be specified without specifying maintenance-domain name.

Required Privilege Level

view

RELATED DOCUMENTATION

clear oam ethernet connectivity-fault-management policer | 2645

List of Sample Output

show oam ethernet connectivity-fault-management policer on page 2783
show oam ethernet connectivity-fault-management policer maintenance-domain md-name on page 2784
show oam ethernet connectivity-fault-management policer maintenance-domain md-name maintenance-association ma-name on page 2784

Output Fields

Table 245 on page 2783 lists the output fields for the **show oam ethernet connectivity-fault-management policer** command. Output fields are listed in the approximate order in which they appear.

Table 245: show oam ethernet connectivity-fault-management policer Output Fields

Field Name	Field Description
Legend for Policer	Describes the symbols used under the **Scope** and **Type** headings: • G - Global scope • S - Service scope • cc - Continuity check (Type)
Maintenance Domain	Displays the maintenance domain name.
Level	Displays the maintenance domain level configured.
Maintenance association	Displays the maintenance association name.
Policer	Displays the policer name.
Type	Policer type. Value **cc** means this policer is used only to police continuity check CFM messages. Value **other** means this policer is used only to police non-continuity check CFM messages. Value **all** means this policer is used to police all CFM messages.
Scope	Policer scope. Displays whether the *global* (G) policer configuration is applicable or the session (S) specific policer config is applicable.
Drop count	Displays the number of packets dropped by the indicated policer.

Sample Output

show oam ethernet connectivity-fault -management policer

Displays the policer information for all maintenance associations and their maintenance domains.

```
show oam ethernet connectivity-fault-management policer
```

```
Legend for Policer
G - Global scope
S - Service scope
cc - Continuity check
```

```
Maintenance Domain: md1 Level: 1
Maintenance association Policer      Type    Scope Drop count
  ma1                   cfm-policer1 all     G            300
  ma1-2                 cfm-policer1 cc      S            259
  ma1-2                 cfm-policer1 other   G            300
Maintenance Domain: md2 Level: 2
Maintenance association Policer      Type    Scope Drop count
  ma2                   cfm-policer1 cc      G            300
  ma2                   cfm-policer2 other   S            223
```

show oam ethernet
connectivity-fault
-management
policer
maintenance-domain
md-name

Displays the policer information for the specified maintenance domain and its maintenance associations.

`show oam ethernet connectivity-fault-management policer maintenance-domain md1`

```
Legend for Policer
G - Global scope
S - Service scope
cc - Continuity check

Maintenance Domain: md1 Level: 1
Maintenance association Policer      Type    Scope Drop count
  ma1                   cfm-policer1 all     G            300
  ma1-2                 cfm-policer1 cc      S            259
  ma1-2                 cfm-policer1 other   G            300
```

show oam ethernet
connectivity-fault
-management
policer
maintenance-domain
md-name
maintenance-association
ma-name

Displays the policer information for the specified **maintenance-domain** ***md-name*** and **maintenance-association** ***ma-name***.

```
show oam ethernet connectivity-fault-management policer maintenance-domain
md5 maintenance-association ma5
```

```
Legend for Policer
G - Global scope
S - Service scope
cc - Continuity check

Maintenance Domain: md5 Level: 5
Maintenance association Policer       Type    Scope Drop count
  ma5                   cfm-policer   cc      S            187
  ma5                   cfm-policer-2 other   S            234
```

show oam ethernet connectivity-fault-management sla-iterator-statistics

Syntax

```
show oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-domain md-name
maintenance-association ma-name
sla-iterator sla-iterator
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 9.6.
Command introduced in Junos OS Release 12.2 for ACX Series routers.
Command introduced in Junos OS Release 13.2 for MX Series routers (not on MPC3E Hyperion cards).

Description

Display the Ethernet Operation, Administration, and Maintenance (OAM) service-level agreement (SLA) iterator statistics.

Options

maintenance-domain *md-name*—Name of an existing connectivity fault management (CFM) maintenance domain.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

sla-iterator *sla-iterator*— Name of the iterator profile.

local-mep *local-mep-id*—(Optional) Numeric identifier of the local MEP. The range of values is **1** through **8191**.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. The range of values is **1** through **8192**.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring an Iterator Profile on a Switch (CLI Procedure) | **341**

clear oam ethernet connectivity-fault-management sla-iterator-statistics | **2636**

List of Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics on page 2790
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) on page 2790
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM)in Metro Ethernet Forum (MEF) mode on page 2792
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) in Metro Ethernet Forum (MEF) mode on page 2793
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay measurement (DM) statistics in non-Metro Ethernet Forum (MEF) mode on page 2795
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) statistics in non-Metro Ethernet Forum (MEF) mode on page 2795
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM) with “legacy-pm-display” option in enhanced-cfm mode on page 2796
show oam ethernet connectivity-fault-management state - To verify the Connectivity Fault Management (CFM) state on page 2797

Output Fields

Table 238 on page 2715 lists the output fields for the **show oam ethernet connectivity-fault-management sla-iterator-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 246: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields

Output Field Name	Output Field Description
Maintenance domain	Name of the maintenance domain.
Level	Level of the maintenance domain level configured.
Maintenance association	Name of the maintenance association.
Local MEP id	Numeric identifier of the local MEP.
Remote MEP id	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
Iterator name	Name of iterator.
Iterator Id	Numeric identifier of the iterator.
Iterator cycle time	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
Iteration period	Maximum number of cycles per iteration
Iterator status	Current status of iterator whether running or stopped.

Table 246: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

Output Field Name	Output Field Description
Infinite iterations	Status of iteration as infinite or finite.
Counter reset time	Date and time when the counter was reset.
Reset reason	Reason to reset counter.
Delay weight	Calculation weight of delay.
Delay variation weight	Calculation weight of delay variation.
DMM sent	Delay measurement message (DMM) PDU frames sent to the peer MEP in this session.
DMM skipped for threshold hit	Number of DMM frames sent to the peer MEP in this session skipped during threshold hit.
DMM skipped for threshold hit window	Number of DMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
DMR received	Number of delay measurement reply (DMR) frames received.
DMR out of sequence	Total number of DMR out of sequence packets received.
DMR received with invalid time stamps	Total number of DMR frames received with invalid timestamps.
Average two-way delay	Average two-way frame delay for the statistics displayed.
Average two-way delay variation	Average two-way “frame jitter” for the statistics displayed.
Average one-way forward delay variation	Average one-way forward delay variation for the statistics displayed in microseconds.
Average one-way backward delay variation	Average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average two-way delay	Weighted average two-way delay for the statistics displayed in microseconds.
Weighted average two-way delay variation	Weighted average two-way delay variation for the statistics displayed in microseconds.

Table 246: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

Output Field Name	Output Field Description
Weighted average one-way backward delay variation	Weighted average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average one-way forward delay variation	Weighted average one-way forward delay variation for the statistics displayed in microseconds.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLM packets received	Total number of synthetic loss message (SLM) PDU frames that the remote MEP received from the source MEP during this ETH-SLM session.
SLR packets sent	Total number of synthetic loss reply (SLR) PDU frames that the remote MEP sent to the source MEP during this measurement session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames that the source MEP received from the remote MEP during this measurement session.
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

show oam ethernet connectivity-fault -management sla-iterator-statistics

`user@switch>` **show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 2**

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i1, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap

Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent                                          : 23898520
DMM skipped for threshold hit                     : 11000
DMM skipped for threshold hit window              : 0
DMR received                                      : 23851165
DMR out of sequence                               : 1142
DMR received with invalid time stamps             : 36540
Average two-way delay                             : 129 usec
Average two-way delay variation                   : 15 usec
Average one-way forward delay variation           : 22 usec
Average one-way backward delay variation          : 22 usec
Weighted average two-way delay                    : 134 usec
Weighted average two-way delay variation          : 8 usec
Weighted average one-way forward delay variation  : 6 usec
Weighted average one-way backward delay variation : 2 usec
```

Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers)

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain mdu maintenance-association mau local-mep 4 remote-mep 3 sla-iterator lm**

```
Iterator statistics:
  Maintenance domain: 2, Level: 2
  Maintenance association: W-160432000-001, Local MEP id: 2
  Remote MEP id: 1, Remote MAC address: 00:90:69:0a:43:39
  Iterator name: iter1, Iterator Id: 1
  Iterator cycle time: 100ms, Iteration period: 10 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2012-09-25 02:15:31 PDT (00:00:45 ago)
  Reset reason: Adjacency flap
  Iterator loss measurement statistics:
    LMM sent                            : 444
    LMM skipped for threshold hit       : 0
    LMM skipped for threshold hit window: 0
    LMR received                        : 444
    LMR out of sequence                 : 0
    LMR forwarding-class mismatch       : 0
  Accumulated transmit statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)                       : 0
  Accumulated receive statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)                       : 0
  Accumulated loss statistics:
    Near-end loss (CIR)                 : 0
    Near-end loss-ratio (CIR)           : 0 (0.00000%)
    Far-end loss (CIR)                  : 0
    Far-end loss-ratio (CIR)            : 0 (0.00000%)
    Near-end loss (CIR)                 : 0
    Near-end loss-ratio (EIR)           : 0 (0.00000%)
    Far-end loss (CIR)                  : 0
    Far-end loss-ratio (EIR)            : 0 (0.00000%)
  Last loss measurement statistics:
    Near-end (CIR)                      : 0
    Far-end (CIR)                       : 0
    Near-end (EIR)                      : 0
    Far-end (EIR)
```

Sample Output

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM)in Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator DM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM, Iterator Id: 1
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:48:23 PST (00:00:54 ago)
  Reset reason: Adjacency flap
  Current delay measurement statistics:
    Measurement Interval Index                : 2 (Suspect status : 1)
    Measurement Interval Start Time           : 2018-12-05 19:48:23 PST (Elapsed
 time : 53011 msec)
    Frame Delay two way (min, max, avg)       : 251 , 295 , 262  (usec)
    Frame Delay forward (min, max, avg)       : 125 , 147 , 131  (usec)
    Frame Delay backward (min, max, avg)      : 125 , 147 , 131  (usec)
    Inter Frame Delay two way (min, max, avg) : 0 , 42 , 7  (usec)
    Inter Frame Delay forward (min, max, avg) : 0 , 21 , 3  (usec)
    Inter Frame Delay backward (min, max, avg) : 0 , 21 , 3  (usec)
    Frame Delay Range two way (max, avg)      : 0 , 0  (usec)
    Frame Delay Range forward (max, avg)      : 0 , 0  (usec)
    Frame Delay Range backward (max, avg)     : 0 , 0  (usec)
    SOAM TXed                                 : 52
    SOAM RXed                                 : 52

  Delay measurement bin statistics:
    Measurement Interval Index     : 2
    Two Way Frame Delay
       [0           - 4999       ] (usec)   : 52
       [5000        - 9999       ] (usec)   : 0
       [10000       - Infinity   ] (usec)   : 0
    Forward Frame Delay
       [0           - 4999       ] (usec)   : 52
       [5000        - 9999       ] (usec)   : 0
       [10000       - Infinity   ] (usec)   : 0
    Backward Frame Delay
       [0           - 4999       ] (usec)   : 52
```

```
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Two Way Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Forward Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Backward Inter Frame Delay Variation
      [0           - 4999       ] (usec)   : 51
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Two Way Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Forward Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
   Backward Frame Delay Range
      [0           - 4999       ] (usec)   : 0
      [5000        - 9999       ] (usec)   : 0
      [10000       - Infinity   ] (usec)   : 0
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) in Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator SLM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_SLM, Iterator Id: 2
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:48:23 PST (00:00:11 ago)
  Reset reason: Adjacency flap
  Iterator synthetic loss measurement statistics:
```

```
   SLM skipped for threshold hit        : 0
   SLM skipped for threshold hit window : 0
   SLR out of sequence                  : 0
   SLM Sample Size                      : 180 SLMs
   Local packet Stats (TxFCl, RxFCl)    : 11, 11
   Last SLR packet stats (TxFCf, TxFCb) : 11, 11
   Last measured FLR (fwd, bkwd)        : 0.000%, 0.000% (Sample #NA)


 Current Measurement Interval loss statistics:
   Measurement Interval Index           : 2 (Suspect Status: 1)
   Measurement Interval Start Time      : 2018-12-05 19:48:23 PST (Elapsed time:
10042 msec)
   SOAM Frames (Tx, Rx)                 : 10, 10
   Forward Frame Stats (Tx, Rx)         : 10, 10
   Backward Frame Stats (Tx, Rx)        : 10, 10
   Frame Loss (fwd, bkwd)               : 0, 0
   Forward FLR minimum                  : 0.000%
   Forward FLR maximum                  : 0.000%
   Forward FLR average                  : 0.000%
   Backward FLR minimum                 : 0.000%
   Backward FLR maximum                 : 0.000%
   Backward FLR average                 : 0.000%

 Current Measurement Interval availability statistics:
   Measurement Interval Index           : 2 (Suspect Status: 1)
   Measurement Interval Start Time      : 2018-12-05 19:48:23 PST (Elapsed time:
10042 msec)
   High loss (fwd, bkwd)                : 0 , 0
   Consecutive high loss (fwd, bkwd)    : 0 , 0
   Available (fwd, bkwd)                : 0 , 0
   Unavailable (fwd, bkwd)              : 0 , 0
   Forward FLR minimum                  : 0.000%
   Forward FLR maximum                  : 0.000%
   Forward FLR average                  : 0.000%
   Backward FLR minimum                 : 0.000%
   Backward FLR maximum                 : 0.000%
   Backward FLR average                 : 0.000%

   Last known available status  (fwd, bkwd)    : unknown, unknown
   Last known forward availability transition  : NA
   Last known backward availability transition : NA
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay measurement (DM) statistics in non-Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator DM**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM, Iterator Id: 1
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:43:47 PST (00:02:44 ago)
  Reset reason: Adjacency flap
  Iterator delay measurement statistics:
    Calculation weight: Delay: 1, Delay variation: 1
    DMM sent                                        : 164
    DMM skipped for threshold hit                   : 0
    DMM skipped for threshold hit window            : 0
    DMR received                                    : 164
    DMR out of sequence                             : 0
    DMR forwarding-class mismatch                   : 0
    DMR received with invalid time stamps           : 0
    Average two-way delay                           : 234 usec
    Average two-way delay variation                 : 9 usec
    Average one-way forward delay variation         : 346 usec
    Average one-way backward delay variation        : 346 usec
    Weighted average two-way delay                  : 221 usec
    Weighted average two-way delay variation        : 2 usec
    Weighted average one-way forward delay variation : 357 usec
    Weighted average one-way backward delay variation: 355 usec
    Bestcase two-way delay                          : 210 usec
    Worstcase two-way delay                         : 283 usec
    Weighted Bestcase two-way delay                 : 210 usec
    Weighted Worstcase two-way delay                : 283 usec
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Synthetic loss measurement (SLM) statistics in non-Metro Ethernet Forum (MEF) mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator SLM**

```
Iterator statistics:
```

```
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_SLM, Iterator Id: 2
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:43:47 PST (00:03:23 ago)
  Reset reason: Adjacency flap
  Iterator synthetic loss measurement statistics:
    SLM sent                            : 202
    SLM skipped for threshold hit       : 0
    SLM skipped for threshold hit window: 0
    SLR received                        : 202
    SLR out of sequence                 : 0
  SLM  transmit statistics:
    SLM TXed                            : 202
    SLM RXed                            : 202
    SLM Last packet Tx count            : 202
    SLM Last packet Rx count            : 202
  Last loss measurement statistics:
    Near-end loss                       : 0 (0.00%)
    Far-end  loss                       : 0 (0.00%)
```

show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) - Delay Measurement (DM) with “legacy-pm-display” option in enhanced-cfm mode

`user@router>` **show oam ethernet connectivity-fault-management sla-iterator-statistics maintenance-domain md6-1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator Legacy**

```
Iterator statistics:
  Maintenance domain: md6-1, Level: 6
  Maintenance association: ma1, Local MEP id: 1
  Remote MEP id: 2, Remote MAC address: 00:23:9c:db:0d:7a
  Iterator name: Test_DM_Legacy, Iterator Id: 3
  Iterator cycle time: 1000ms, Iteration period: 2000 cycles
  Iterator status: running, Infinite iterations: true
  Counter reset time: 2018-12-05 19:51:33 PST (00:00:15 ago)
  Reset reason: Adjacency flap
  Iterator delay measurement statistics:
    Calculation weight: Delay: 1, Delay variation: 1
    DMM sent                                        : 14
    DMM skipped for threshold hit                   : 0
    DMM skipped for threshold hit window            : 0
```

```
    DMR received                                    : 14
    DMR out of sequence                             : 0
    DMR forwarding-class mismatch                   : 0
    DMR received with invalid time stamps           : 0
    Average two-way delay                           : 324 usec
    Average two-way delay variation                 : 7 usec
    Average one-way forward delay variation         : 240 usec
    Average one-way backward delay variation        : 240 usec
    Weighted average two-way delay                  : 324 usec
    Weighted average two-way delay variation        : 6 usec
    Weighted average one-way forward delay variation : 222 usec
    Weighted average one-way backward delay variation: 222 usec
    Bestcase two-way delay                          : 312 usec
    Worstcase two-way delay                         : 333 usec
    Weighted Bestcase two-way delay                 : 312 usec
    Weighted Worstcase two-way delay                : 333 usec
```

show oam ethernet connectivity-fault-management state - To verify the Connectivity Fault Management (CFM) state

The following command is to verify whether the CFM state is in enhanced-cfm mode or not.

`user@router>` **show oam ethernet connectivity-fault-management state**

```
Connectivity fault management state:
    CFM Mode Of Operation: Enhanced
    Enhanced IP Mode: Enabled
    CFM Config State: Ok
    CFM Cleanup State: Ok
    CFM Restart Timer State: Cleanup Timer State stopped Rebooting in 0 sec
    CFM CFMMAN Job State: Not Pending
    Number of sessions: 1
    Number of sessions created: 1
    Number of sessions deleted: 0
    Number of sessions freed: 0
    Number of sessions enqueued: 1
    Number of sessions dequeued: 1
    VPLS feature: enabled
    Token based forwarding feature: enabled
    Forwarding table filtering simulation feature: disabled
    Hardware assisted flooding feature: enabled
    Flood resynchronization for GRES feature: enabled
    Shared interface filter feature: disabled
    Hardware timestamping feature: disabled
```

```
    Marking of connection protection TLV feature: disabled
    CFMD config memory resource  limit(in bytes): 3221225472
    CFMD max resident set (peak) size (in bytes):  24158208

Packet processing state:
    State of the connection to packet processing daemon: down
    State of the flow to packet processing daemon: ready
    State of the packet processing job: ready
    Number of times the connection to packet processing daemon was blocked: 0
    State of the connection to cfmman: slots: 2 3 4 5

Filter state:
    State of the connection to firewall daemon: Connected
    Number of reconnects made to firewall daemon: 0
    Number of requests sent to firewall daemon: 13
    Number of requests accepted by firewall daemon: 13
    Number of requests rejected by firewall daemon: 0
    Number of requests lost due to disconnection: 0
```

show oam ethernet connectivity-fault-management synthetic-loss-statistics

Syntax

```
show oam ethernet connectivity-fault-management synthetic-loss-statistics
<local-mep local-mep-id>
maintenance-association ma-name
<count entry-count>
maintenance-domain md-name
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 13.2 for MX Series routers.

Description

On MX Series routers with Modular Port Concentrators (MPCs) with Ethernet interfaces, display the on-demand ETH-SLM statistics.

Options

count *entry-count*—(Optional) Number of entries to display from the statistics table. The range of values is from 1 through 100. The default value is 100.

local-mep *local-mep-id*—(Optional) Numeric identifier of the local MEP. The range of values is from **1** through **8192**.

maintenance-association *ma-name*—Name of an existing CFM maintenance association.

maintenance-domain *md-name*—Name of an existing connectivity fault management (CFM) maintenance domain.

remote-mep *remote-mep-id*—(Optional) Numeric identifier of the remote MEP. The range of values is from **1** through **8192**.

Required Privilege Level

view

RELATED DOCUMENTATION

- clear oam ethernet connectivity-fault-management statistics | 2647
- clear oam ethernet connectivity-fault-management synthetic-loss-measurement | 2649
- show oam ethernet connectivity-fault-management interfaces | 2727
- show oam ethernet connectivity-fault-management mep-database | 2749
- show oam ethernet connectivity-fault-management mep-statistics | 2764

List of Sample Output

show oam ethernet connectivity-fault-management synthetic-loss-statistics on page 2801

Output Fields

Table 247 on page 2800 lists the output fields for the **show oam ethernet connectivity-fault-management synthetic-loss-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 247: show oam ethernet connectivity-fault-management synthetic-loss-statistics Output Fields

Output Field Name	Field Description
MEP identifier	Maintenance association end point (MEP) numeric identifier.
MAC address	Unicast MAC address configured for the MEP.
Remote MEP count	Number of remote MEPs (unless you specify the **remote-mep** option).
Remote MEP identifier	Numeric identifier of the remote MEP.
Remote MAC address	Unicast MAC address of the remote MEP.
SLM packets sent	Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.
SLM packets received	Total number of synthetic loss message (SLM) PDU frames that the remote MEP received from the source MEP during this ETH-SLM session.
SLR packets sent	Total number of synthetic loss reply (SLR) PDU frames that the remote MEP sent to the source MEP during this measurement session.
SLR packets received	Total number of synthetic loss reply (SLR) PDU frames that the source MEP received from the remote MEP during this measurement session.
Local TXFC1 value	Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.
Local RXFC1 value	Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TxFC1 is sent in the packet.
Last Received SLR frame TXFCf(tc)	Value of the local counter TxFCl at the time of SLM frame transmission.

Table 247: show oam ethernet connectivity-fault-management synthetic-loss-statistics Output Fields *(continued)*

Output Field Name	Field Description
Last Received SLR frame TXFCb(t	Value of the local counter RxFCl at the time of SLR frame transmission.
Frame loss (near-end)	Count of frame loss associated with ingress data frames.
Frame loss (far-end)	Count of frame loss associated with egress data frames.

Sample Output

show oam ethernet connectivity-fault-management synthetic-loss-statistics

`user@switch>` **show oam ethernet connectivity-fault-management synthetic-loss-statistics maintenance-domain md6 maintenance-association ma6**

```
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count: 2
  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
  Synthetic Loss measurement statistics:
   SLM packets sent                          : 100
   SLM packets received                      : 0
   SLR packets sent                          : 100
   SLR packets received                      : 0
  Accumulated SLM statistics:
   Local TXFC1 value                         : 100
   Local RXFC1 value                         : 100
   Last Received SLR frame TXFCftc           : 100
   Last Received SLR frame TXFCbtc           : 100
  SLM Frame Loss:
   Frame Loss (far-end)                      : 0 (0.00 %)
   Frame Loss (near-end)                     : 0 (0.00 %)
```

show oam ethernet evc

Syntax

```
show oam ethernet evc <evc-id>
```

Release Information

Command introduced in Junos OS Release 9.5.

Description

On MX Series routers with OAM Ethernet Virtual Connection (EVC) configurations, displays the EVC configuration and status information.

Options

This command has no options.

Required Privilege Level

View

Output Fields

Table 248 on page 2802 lists the output fields for the **show oam ethernet evc** command. Output fields are listed in the approximate order in which they appear.

Table 248: show oam ethernet evc Output Fields

Field Name	Field Description
EVC identifier	Header for the EVC information showing the EVC name, configuration, and active/inactive status.
UNI count	Number of configured and active UNIs.
Protocol	Protocol configured between the UNIs.
Local UNIs	Heading for the list of local UNIs
UNI Identifier	Name of the UNI.
Interface	Interface type-dpc/pic/port.unit-number.
Status	Status operational or not operational.

Sample Output

show oam ethernet evc

user@host> **show oam ethernet evc**

```
EVC identifier: evc1, Point-to-Point, Active
  UNI count: Configured(2), Active(2)
  Protocol: cfm, Management domain: md, Management association: ma
  Local UNIs:
    UNI Identifier      Interface     Status
    uni1                ge-1/1/1      Operational
    uni2                ge-1/1/1      Not Operational
```

show oam ethernet fnp interface

Syntax

show oam ethernet fnp interface
<*ethernet-interface-name*>
<routing-instance *routing-instance-name*>

Release Information

Command introduced in Junos OS Release 11.4.

Description

On MX Series routers with Gigabit Ethernet, Fast Ethernet, or aggregated Ethernet PICs, displays OAM Ethernet Failure Notification Protocol (FNP) information for Ethernet interfaces.

Options

interface-name—(Optional) Display Ethernet FNP information for the specified Ethernet interface only.

routing-instance-name—(Optional) Display FNP for the specified routing instance.

Required Privilege Level

view

List of Sample Output

show oam ethernet fnp interface on page 2805

Output Fields

Table 249 on page 2804 lists the output fields for the **show oam ethernet fnp interface** command. Output fields are listed in the approximate order in which they appear.

Table 249: show oam ethernet fnp interface Output Fields

Field Name	Field Description
Interface	Name of the interface for the displayed information.
VLAN	Name of the VLAN.
State	Displays state of the interface.
FNP Message Interface	Displays the message interface type.
FNP Message Source MAC	Displays the source MAC address.

Sample Output

show oam ethernet fnp interface

```
user@host> show oam ethernet fnp interface
```

```
The FNP controlled interfaces are:
Interface   VLAN   State   FNP message   FNP message
                           Interface     Source MAC

ge-0/0/0.30  30     down   lsi.1054976   a0:aa:aa:aa:aa:aa
ge-0/0/0.20  20     down   lsi.1054976   a0:aa:aa:aa:aa:aa
```

show oam ethernet fnp messages

Syntax

```
show oam ethernet fnp messages
<interface interface-name>
<routing instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4

Description

On MX Series routers with Gigabit Ethernet, Fast Ethernet, or aggregated Ethernet PICs, displays OAM Ethernet Failure Notification Protocol (FNP) messages.

Options

interface-name—(Optional) Display Ethernet FNP messages for the specified Ethernet interface only.

routing-instance-name—(Optional) Display FNP messages for the specified routing instance.

Required Privilege Level

view

List of Sample Output

show oam ethernet fnp messages on page 2807

Output Fields

Table 250 on page 2806 lists the output fields for the **show oam ethernet fnp messages** command. Output fields are listed in the approximate order in which they appear.

Table 250: show oam ethernet fnp messages Output Fields

Field Name	Field Description
Message from source MAC address	The source MAC address of the message.
Originating port number	Port number of the original message.
Time since last message	Elapsed time in hours, minutes, and seconds since the last message was received.
Time since last message update	Elapsed time in hours, minutes, and seconds since the last message was updated.
Total messages received	Number of messages received.

Table 250: show oam ethernet fnp messages Output Fields *(continued)*

Field Name	Field Description
Domain ID	Domain ID of the message.
STP Root ID	The spanning tree Root ID of the message.
Trigger Reason	The reason why the message was triggered.
Effected VLANs	Number of VLANs that are affected.
Disabled interfaces	Name of the interfaces that are disabled.

Sample Output

show oam ethernet fnp messages

`user@host>` **show oam ethernet fnp messages**

```
Active FNP messages on interface lsi.1054465
Message source MAC: a0:aa:aa:aa:aa:aa
  Originating port number: 141077
  Time since last message: 00:00:00
  Time since last message update: 00:00:00
  Total messages received: 1
  Domain ID: 0
  STP Root ID: 0.f0:ff:ff:ff:ff:ff
  Trigger reason: todo
  Effected VLANs: 10
  Disabled interfaces:
    Interface VLAN
    ge-0/0/0.10 10
```

show oam ethernet fnp status

Syntax

```
show oam ethernet fnp status
<interface interface-name>
<routing instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4

Description

On MX Series routers with Gigabit Ethernet, Fast Ethernet, or aggregated Ethernet PICs, displays OAM Ethernet Failure Notification Protocol (FNP) status.

Options

interface-name—(Optional) Display Ethernet FNP information for the specified Ethernet interface only.

routing-instance-name—(Optional) Display FNP for the specified routing instance.

Required Privilege Level

view

List of Sample Output

show oam ethernet fnp status on page 2809

Output Fields

Table 251 on page 2808 lists the output fields for the **show oam ethernet fnp status** command. Output fields are listed in the approximate order in which they appear.

Table 251: show oam ethernet fnp status Output Fields

Field Name	Field Description
FNP interval	The time interval between messages.
Loss threshold	The number of messages that can be lost before FNP is marked as down.
FNP enabled interfaces	Displays interfaces that are enabled.
Interface	The name of the interface.
Domain ID	Domain ID of the message.
STP Root ID	The spanning tree Root ID of the message.

Table 251: show oam ethernet fnp status Output Fields *(continued)*

Field Name	Field Description
FNP Messages	The total number of messages received.

Sample Output

show oam ethernet fnp status

`user@host>` **show oam ethernet status**

```
FNP interval:
Loss threshold
FNP enabled interfaces
Interface      Domain ID      STP Root ID              FNP Messages
ge-0/0/0.1278        100      0.f0:ff:ff:ff:ff:ff                 0
```

show oam ethernet lmi

Syntax

```
show oam ethernet lmi (interface <interface-name>)
```

Release Information

Command introduced in Junos OS Release 9.5.

Description

On routers with Gigabit Ethernet, Fast Ethernet, or aggregated Ethernet, and OAM Ethernet Local Management Interface (E-LMI) configuration, display the LMI information for the configured interfaces or optionally for a specified interface.

> **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

interface—(Optional) Display LMI information for a specified interface.

interface-name—(Optional) Display Ethernet LMI information for the specified interface only.

Required Privilege Level

View

Output Fields

Table 252 on page 2810 lists the output fields for the **show oam ethernet lmi** command. Output fields are listed in the approximate order in which they appear.

Table 252: show oam ethernet lmi Output Fields

Field Name	Field Description
Physical Interface	Header for the EVC information showing the Ethernet virtual circuit (EVC) name, configuration, and active/inactive status.
UNI Identifier	Name of the UNI.
EVC map type	EVC configuration.
Polling verification timer	Polling verification timer status.

Table 252: show oam ethernet lmi Output Fields *(continued)*

Field Name	Field Description
E-LMI state	Operational status of the E-LMI configuration in the interfaces or specified interface.
Priority/Untagged VLAN ID	To be provided.
Default EVC	The EVC set as the default EVC.
Associated EVCs	Heading for the list of configured EVCs.
EVC Indentifier	EVC name.
Reference ID	To be provided.
Status	Status active or not active.
CE VLAN IDs	Customer edge VLAN ID numbers.

Sample Output

show oam ethernet lmi interface

`user@host>` **show oam ethernet lmi interface ge-1/1/1**

```
Physical interface: ge-1/1/1, Physical link is Up
  UNI identifier: uni-ce1, EVC map type: Bundling
  Polling verification timer: Enabled, E-LMI state: Operational
  Priority/Untagged VLAN ID: 20, Default EVC: evc1
  Associated EVCs:
    EVC         Reference     Status           CE VLAN IDs
    Identifier  ID
    evc1            1        Active (New)        1-2048
    evc2             2        Not Active          2049-4096
```

show oam ethernet lmi statistics

Syntax

```
show oam ethernet lmi statistics <interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.5.

Description

On MX Series routers with Gigabit Ethernet, Fast Ethernet, or aggregated Ethernet PICs, displays OAM Ethernet Local Management Interface (LMI) statistics.

Options

interface—(Optional) Display LMI statistics for a specified interface.

interface-name—(Optional) Display Ethernet LMI information for the specified Ethernet interface only.

Required Privilege Level

view

List of Sample Output

show oam ethernet lmi statistics on page 2813

Output Fields

Table 253 on page 2812 lists the output fields for the **show oam ethernet lmi statistics** command. Output fields are listed in the approximate order in which they appear.

Table 253: show oam ethernet lmi statistics Output Fields

Field Name	Field Description
Physical interface	Name of the interface for the displayed statistics.
Reliability errors	Number of E-LMI reliability errors logged.
Protocol errors	Number of E-LMI protocol errorse.
Status check received	Number of E-LMI status check receive errors.
Status check sent	Number of E-LMI status check sent errors.
Full status received	Number of E-LMI full status receive errors.
Full status sent	Number of E-LMI full status sent errors.

Table 253: show oam ethernet lmi statistics Output Fields *(continued)*

Field Name	Field Description
Full status continued received	Number of E-LMI status continued received errors.
Full status continued sent	Number of E-LMI full status continued sent errors.
Asynchronous status sent	Number of E-LMI asynchronous status sent errors.

Sample Output

show oam ethernet lmi statistics

`user@host>` **show oam ethernet lmi statistics interface ge-1/1/1**

```
Physical interface: ge-1/1/1
  Reliability errors                     4  Protocol errors
0
  Status check received                  0  Status check sent
0
  Full status received                 694  Full status sent                694

  Full status continued received         0  Full status continued sent
0
  Asynchronous status sent               0
```

CHAPTER 83

Operational Commands: Ethernet OAM Link Fault Management

IN THIS CHAPTER

- show oam ethernet link-fault-management | **2815**
- show oam ethernet link-fault-management | **2822**
- clear oam ethernet link-fault-management state | **2832**
- clear oam ethernet link-fault-management statistics | **2833**

show oam ethernet link-fault-management

Syntax

```
show oam ethernet link-fault-management
<brief | detail>
<interface-name>
```

Release Information

Command introduced in Junos OS Release 9.4 for EX Series switches.

Description

Displays Operation, Administration, and Maintenance (OAM) link fault management (LFM) information for Ethernet interfaces.

Options

brief | detail—(Optional) Display the specified level of output.

interface-name —(Optional) Display link fault management information for the specified Ethernet interface only.

Required Privilege Level

view

RELATED DOCUMENTATION

Example: Configuring Ethernet OAM Link Fault Management | 331

Configuring Ethernet OAM Link Fault Management | 329

List of Sample Output

show oam ethernet link-fault-management brief on page 2820

show oam ethernet link-fault-management detail on page 2820

Output Fields

Table 254 on page 2816 lists the output fields for the **show oam ethernet link-fault-management** command. Output fields are listed in the approximate order in which they appear.

Table 254: show oam ethernet link-fault-management Output Fields

Field Name	Field Description	Level of Output
Status	Indicates the status of the established link. • **Fail**—A link fault condition exists. • **Running**—A link fault condition does not exist.	All levels
Discovery state	State of the discovery mechanism: • **Passive Wait** • **Send Any** • **Send Local Remote** • **Send Local Remote Ok**	All levels
Peer address	Address of the OAM peer.	All levels
Flags	Information about the interface. • **Remote-Stable**—Indicates remote OAM client acknowledgment of, and satisfaction with local OAM state information. **False** indicates that remote DTE has either not seen or is unsatisfied with local state information. **True** indicates that remote DTE has seen and is satisfied with local state information. • **Local-Stable**—Indicates local OAM client acknowledgment of, and satisfaction with remote OAM state information. **False** indicates that local DTE either has not seen or is unsatisfied with remote state information. **True** indicates that local DTE has seen and is satisfied with remote state information. • **Remote-State-Valid**—Indicates the OAM client has received remote state information found within Local Information TLVs of received Information OAM PDUs. **False** indicates that OAM client has not seen remote state information. **True** indicates that the OAM client has seen remote state information.	All levels
Remote loopback status	Indicates the remote loopback status. An OAM entity can put its remote peer into loopback mode using the Loopback control OAM PDU. In loopback mode, every frame received is transmitted back on the same port (except for OAM PDUs, which are needed to maintain the OAM session).	All levels

Table 254: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote entity information	Remote entity information. • **Remote MUX action**—Indicates the state of the multiplexer functions of the OAM sublayer. Device is forwarding non-OAM PDUs to the lower sublayer or discarding non-OAM PDUs. • **Remote parser action**—Indicates the state of the parser function of the OAM sublayer. Device is forwarding non-OAM PDUs to higher sublayer, looping back non-OAM PDUs to the lower sublayer, or discarding non-OAM PDUs. • **Discovery mode**—Indicates whether discovery mode is active or inactive. • **Unidirectional mode**—Indicates the ability to operate a link in a unidirectional mode for diagnostic purposes. • **Remote loopback mode**—Indicates whether remote loopback is supported or not supported. • **Link events**—Indicates whether interpreting link events is supported or not supported on the remote peer. • **Variable requests**—Indicates whether variable requests are supported or not supported. The Variable Request OAM PDU, is used to request one or more MIB variables from the remote peer.	All levels
OAM Receive Statistics		
Information	The number of information PDUs received.	**detail**
Event	The number of loopback control PDUs received.	**detail**
Variable request	The number of variable request PDUs received.	**detail**
Variable response	The number of variable response PDUs received.	**detail**
Loopback control	The number of loopback control PDUs received.	**detail**
Organization specific	The number of vendor organization specific PDUs received.	**detail**
OAM Transmit Statistics		
Information	The number of information PDUs transmitted.	**detail**
Event	The number of event notification PDUs transmitted.	**detail**

Table 254: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Variable request	The number of variable request PDUs transmitted.	**detail**
Variable response	The number of variable response PDUs transmitted.	**detail**
Loopback control	The number of loopback control PDUs transmitted.	**detail**
Organization specific	The number of vendor organization specific PDUs transmitted.	**detail**
OAM Received Symbol Error Event information		
Events	The number of symbol error event TLVs that have been received after the OAM sublayer was reset.	**detail**
Window	The symbol error event window in the received PDU. The protocol default value is the number of symbols that can be received in one second on the underlying physical layer.	**detail**
Threshold	The number of errored symbols in the period required for the event to be generated.	**detail**
Errors in period	The number of symbol errors in the period reported in the received event PDU.	**detail**
Total errors	The number of errored symbols that have been reported in received event TLVs after the OAM sublayer was reset. Symbol errors are coding symbol errors.	**detail**
OAM Received Frame Error Event Information		
Events	The number of errored frame event TLVs that have been received after the OAM sublayer was reset.	**detail**
Window	The duration of the window in terms of the number of 100 ms period intervals.	**detail**
Threshold	The number of detected errored frames required for the event to be generated.	**detail**
Errors in period	The number of detected errored frames in the period.	**detail**

Table 254: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Total errors	The number of errored frames that have been reported in received event TLVs after the OAM sublayer was reset. A frame error is any frame error on the underlying physical layer.	**detail**
OAM Received Frame Period Error Event Information		
Events	The number of frame seconds errors event TLVs that have been received after the OAM sublayer was reset.	**detail**
Window	The duration of the frame seconds window.	**detail**
Threshold	The number of frame seconds errors in the period.	**detail**
Errors in period	The number of frame seconds errors in the period.	**detail**
Total errors	The number of frame seconds errors that have been reported in received event TLVs after the OAM sublayer was reset.	**detail**
OAM Transmitted Symbol Error Event Information		
Events	The number of symbol error event TLVs that have been transmitted after the OAM sublayer was reset.	**detail**
Window	The symbol error event window in the transmitted PDU.	**detail**
Threshold	The number of errored symbols in the period required for the event to be generated.	**detail**
Errors in period	The number of symbol errors in the period reported in the transmitted event PDU.	**detail**
Total errors	The number of errored symbols reported in event TLVs that have been transmitted after the OAM sublayer was reset.	**detail**
OAM Transmitted Frame Error Event Information		
Events	The number of errored frame event TLVs that have been transmitted after the OAM sublayer was reset.	**detail**
Window	The duration of the window in terms of the number of 100 ms period intervals.	**detail**

Table 254: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Threshold	The number of detected errored frames required for the event to be generated.	**detail**
Errors in period	The number of detected errored frames in the period.	**detail**
Total errors	The number of errored frames that have been detected after the OAM sublayer was reset.	**detail**

Sample Output

show oam ethernet link-fault-management brief

```
user@host> show oam ethernet link-fault-management brief
```

```
Interface: ge-0/0/1
  Status: Running, Discovery state: Send Any
  Peer address: 00:90:69:72:2c:83
  Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
  Remote loopback status: Disabled on local port, Enabled on peer port
  Remote entity information:
    Remote MUX action: discarding, Remote parser action: loopback
    Discovery mode: active, Unidirectional mode: unsupported
    Remote loopback mode: supported, Link events: supported
    Variable requests: unsupported
```

show oam ethernet link-fault-management detail

```
user@host> show oam ethernet link-fault-management detail
```

```
  Interface: ge-0/0/1
    Status: Running, Discovery state: Send Any
    Peer address: 00:90:69:0a:07:14
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 186365, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM transmit statistics:
      Information: 186347, Event: 0, Variable request: 0, Variable response: 0
```

```
  Loopback control: 0, Organization specific: 0
OAM received symbol error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM received frame error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM received frame period error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM transmitted symbol error event information:
  Events: 0, Window: 0, Threshold: 1
  Errors in period: 0, Total errors: 0
OAM transmitted frame error event information:
  Events: 0, Window: 0, Threshold: 1
  Errors in period: 0, Total errors: 0
Remote entity information:
  Remote MUX action: forwarding, Remote parser action: forwarding
  Discovery mode: active, Unidirectional mode: unsupported
  Remote loopback mode: supported, Link events: supported
  Variable requests: unsupported
```

show oam ethernet link-fault-management

Syntax

```
show oam ethernet link-fault-management
<brief | detail>
<interface-name>
```

Release Information

Command introduced in Junos OS Release 8.2.

Description

On EX Series switches and M320, M120, MX Series, T320, and T640 routers, display Operation, Administration, and Management (OAM) link fault management information for Ethernet interfaces.

Options

brief | detail—(Optional) Display the specified level of output.

interface-name—(Optional) Display link fault management information for the specified Ethernet interface only.

Required Privilege Level

view

List of Sample Output

show oam ethernet link-fault-management brief on page 2828
show oam ethernet link-fault-management brief (Loopback tracking) on page 2828
show oam ethernet link-fault-management detail on page 2829
show oam ethernet link-fault-management detail (backup Routing Engine) on page 2830

Output Fields

Table 254 on page 2816 lists the output fields for the **show oam ethernet link-fault-management** command. Output fields are listed in the approximate order in which they appear.

Table 255: show oam ethernet link-fault-management Output Fields

Field Name	Field Description	Level of Output
Status	Indicates the status of the OAM discovery state mechanism . • **Down**—Discovery mechanism is not running.. • **Running**—Discovery mechanism is running.	All levels

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Discovery state	State of the discovery mechanism. If the status of the discovery mechanism is Down then the state of discovery mechanism is Fault. However, if the status of the discovery mechanism is Running then the state can be any one of the following: • **Passive Wait** • **Active Send Local** • **Send Any** • **Send Local Remote** • **Send Local Remote Ok** • **Fault**	All levels
ISSU	Specifies that the local end is undergoing a unified in-service software upgrade (ISSU).	All levels
Peer address	Address of the OAM peer.	All levels
Flags	Information about the interface. Possible values are described in the "Link Flags" section under *Common Output Fields Description*. • **Remote-Stable**—Indicates remote OAM client acknowledgment of and satisfaction with local OAM state information. **False** indicates that remote DTE either has not seen or is unsatisfied with local state information.**True** indicates that remote DTE has seen and is satisfied with local state information. • **Local-Stable**—Indicates local OAM client acknowledgment of and satisfaction with remote OAM state information. **False** indicates that local DTE either has not seen or is unsatisfied with remote state information. **True** indicates that local DTE has seen and is satisfied with remote state information. • **Remote-State-Valid**—Indicates the OAM client has received remote state information found within Local Information TLVs of received Information OAM PDUs. **False** indicates that OAM client has not seen remote state information. **True** indicates that the OAM client has seen remote state information.	All levels
Remote loopback status	Indicates the remote loopback status. An OAM entity can put its remote peer into loopback mode using the Loopback control OAM PDU. In loopback mode, every frame received is transmitted back on the same port (except for OAM PDUs, which are needed to maintain the OAM session).	All levels

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote entity information	Remote entity information. • **Remote MUX action**—Indicates the state of the multiplexer functions of the OAM sublayer. Device is forwarding non-OAM PDUs to the lower sublayer or discarding non-OAM PDUs. • **Remote parser action**—Indicates the state of the parser function of the OAM sublayer. Device is forwarding non-OAM PDUs to higher sublayer, looping back non-OAM PDUs to the lower sublayer, or discarding non-OAM PDUs. • **Discovery mode**—Indicates whether discovery mode is active or inactive. • **Unidirectional mode**—Indicates the ability to operate a link in a unidirectional mode for diagnostic purposes. • **Remote loopback mode**—Indicates whether remote loopback is supported or unsupported. • **Link events**—Indicates whether interpreting link events is supported or unsupported on the remote peer. • **Variable requests**—Indicates whether variable requests are supported. The Variable Request OAM PDU, is used to request one or more MIB variables from the remote peer. • **Remote in ISSU**—Indicates that the remote end is undergoing a unified in-service software upgrade (ISSU).	All levels
Loopback Tracking	Indicates that loopback detection is enabled or disabled.	All levels
Loop Status	Indicates that a loopback issue is either found, not found, or unknown when loopback tracking is enabled.	All levels
Detect LOC	Indicates that loss-of-continuity (LOC) detection is enabled or disabled.	All levels
LOC status	Indicates that a LOC issue is either found, not found, or unknown when Detect LOC is enabled. Status is unknown when LOC detection is disabled.	All levels
OAM Receive Statistics		
Information	The total number of information PDUs received.	**detail**
Event	The total number of loopback control PDUs received.	**detail**
Variable request	The total number of variable request PDUs received.	**detail**

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Variable response	The total number of variable response PDUs received.	**detail**
Loopback control	The total number of loopback control PDUs received.	**detail**
Organization specific	The total number of vendor organization specific PDUs received.	**detail**
OAM Transmit Statistics		
Information	The total number of information PDUs transmitted.	**detail**
Event	The total number of event notification PDUs transmitted.	**detail**
Variable request	The total number of variable request PDUs transmitted.	**detail**
Variable response	The total number of variable response PDUs transmitted.	**detail**
Loopback control	The total number of loopback control PDUs transmitted.	**detail**
Organization specific	The total number of vendor organization specific PDUs transmitted.	**detail**
OAM Received Symbol Error Event information		
Events	The number of symbol error event TLVs that have been received since the OAM sublayer was reset.	**detail**
Window	The symbol error event window in the received PDU. The protocol default value is the number of symbols that can be received in one second on the underlying physical layer.	**detail**
Threshold	The number of errored symbols in the period required for the event to be generated.	**detail**
Errors in period	The number of symbol errors in the period reported in the received event PDU.	**detail**

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Total errors	The number of errored symbols that have been reported in received event TLVs since the OAM sublayer was reset. Symbol errors are coding symbol errors.	**detail**
OAM Received Frame Error Event Information		
Events	The number of errored frame event TLVs that have been received since the OAM sublayer was reset.	**detail**
Window	The duration of the window in terms of the number of 100 ms period intervals.	**detail**
Threshold	The number of detected errored frames required for the event to be generated.	**detail**
Errors in period	The number of detected errored frames in the period.	**detail**
Total errors	The number of errored frames that have been reported in received event TLVs since the OAM sublayer was reset. A frame error is any frame error on the underlying physical layer.	**detail**
OAM Received Frame Period Error Event Information		
Events	The number of frame seconds errors event TLVs that have been received since the OAM sublayer was reset.	**detail**
Window	The duration of the frame seconds window.	**detail**
Threshold	The number of frame seconds errors in the period.	**detail**
Errors in period	The number of frame seconds errors in the period.	**detail**
Total errors	The number of frame seconds errors that have been reported in received event TLVs since the OAM sublayer was reset.	**detail**
OAM Transmitted Symbol Error Event Information		
Events	The number of symbol error event TLVs that have been transmitted since the OAM sublayer was reset.	**detail**
Window	The symbol error event window in the transmitted PDU.	**detail**

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
Threshold	The number of errored symbols in the period required for the event to be generated.	**detail**
Errors in period	The number of symbol errors in the period reported in the transmitted event PDU.	**detail**
Total errors	The number of errored symbols reported in event TLVs that have been transmitted since the OAM sublayer was reset.	**detail**
OAM Current Symbol Error Event Information		
Events	The number of symbol error TLVs that have been generated regardless of whether the threshold for sending event TLVs has been crossed.	**detail**
Window	The symbol error event window in the transmitted PDU.	**detail**
Threshold	The number of errored symbols in the period required for the event to be generated.	**detail**
Errors in period	The total number of symbol errors in the period reported.	**detail**
Total errors	The number of errored symbols reported in event TLVs that have been generated regardless of whether the threshold for sending event TLVs has been crossed.	**detail**
OAM Transmitted Frame Error Event Information		
Events	The number of errored frame event TLVs that have been transmitted since the OAM sublayer was reset.	**detail**
Window	The duration of the window in terms of the number of 100 ms period intervals.	**detail**
Threshold	The number of detected errored frames required for the event to be generated.	**detail**
Errors in period	The number of detected errored frames in the period.	**detail**
Total errors	The number of errored frames that have been detected since the OAM sublayer was reset.	**detail**

Table 255: show oam ethernet link-fault-management Output Fields *(continued)*

Field Name	Field Description	Level of Output
OAM Current Frame Error Event Information		
Events	The number of errored frame event TLVs that have been generated regardless of whether the threshold for sending event TLVs has been crossed.	**detail**
Window	The duration of the window in terms of the number of 100 ms period intervals.	**detail**
Threshold	The number of detected errored frames required for the event to be generated.	**detail**
Errors in period	The number of errored frames in the period.	**detail**
Total errors	The number of errored frames detected regardless of whether the threshold for transmitting event TLVs has been crossed.	**detail**

Sample Output

show oam ethernet link-fault-management brief

```
user@host> show oam ethernet link-fault-management brief
```

```
Interface: ge-3/1/3
  Status: Running, Discovery state: Send Any, ISSU
  Peer address: 00:90:69:72:2c:83
  Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50  Remote loopback status:
 Disabled on local port, Enabled on peer port
  Remote entity information:
    Remote MUX action: discarding, Remote parser action: loopback
    Discovery mode: active, Unidirectional mode: unsupported
    Remote loopback mode: supported, Link events: supported
    Variable requests: unsupported, Remote in ISSU
```

show oam ethernet link-fault-management brief (Loopback tracking)

```
user@host> show oam ethernet link-fault-management
```

```
Interface: ge-3/1/3
  Status: Running, Discovery state: Active Send Local
  Peer address: 00:00:00:00:00:00
  Flags:0x8
  Loopback tracking: Enabled,      Loop Status: Found
```

show oam ethernet link-fault-management detail

user@host> **show oam ethernet link-fault-management detail**

```
  Interface: ge-6/1/0
    Status: Running, Discovery state: Send Any, ISSU
    Peer address: 00:90:69:0a:07:14
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 186365, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM transmit statistics:
      Information: 186347, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
```

```
      Remote loopback mode: supported, Link events: supported
      Variable requests: unsupported, Remote in ISSU
```

show oam ethernet link-fault-management detail (backup Routing Engine)

`user@host>` **show oam ethernet link-fault-management ge-0/2/0 detail**

```
Interface: ge-0/2/0
    Status: Running, Discovery state: Send Any
    Transmit interval: 100ms, PDU threshold: 3 frames, Hold time: 300ms
    Peer address: ac:4b:c8:81:90:a4
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 786, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
```

```
    Loopback tracking: Enabled, Loop status: Not Found
    Detect LOC: Enabled, LOC status: Not Found
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                   Invoked     Executed
  LK_ADJ_LOSS100_1                         1        1
  LK_ADJ_LOSS100_2                         1        0
  LK_ADJ_LOSS100_3                         1        0
  LK_ADJ_LOSS101_1                         1        1
  LK_ADJ_LOSS101_2                         1        0
  LK_ADJ_LOSS101_3                         1        0
  LK_ADJ_LOSS106_1                         0        0
  LK_ADJ_LOSS106_2                         0        0
  LK_ADJ_LOSS106_3                         0        0
  LK_ADJ_LOSS107_1                         0        0
  LK_ADJ_LOSS107_2                         0        0
  LK_ADJ_LOSS107_3                         0        0
```

clear oam ethernet link-fault-management state

Syntax

```
clear oam ethernet link-fault-management state <interface-name>
```

Release Information

Command introduced in Junos OS Release 8.4.

Description

On all M Series, MX Series, ACX series, PTX Series, T320, and T640 routers, clear link fault management state information, restart the link discovery process, and reset OAM loopback state (if set previously) on Ethernet interfaces.

Options

none—Clear OAM link fault management state information, restart the link discovery process, and reset OAM loopback state (if set previously) on all Ethernet interfaces.

interface-name—(Optional) Clear OAM link fault management state information, restart the link discovery process, and reset OAM loopback state (if set previously) on the specified Ethernet interface only.

Required Privilege Level

view

List of Sample Output

clear oam ethernet link-fault-management state on page 2832

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet link-fault-management state

```
user@host> clear oam ethernet link-fault-management state ge-0/3/3
```

```
Cleared link-fault-management state for interface ge-0/3/3
```

clear oam ethernet link-fault-management statistics

Syntax

```
clear oam ethernet link-fault-management <interface-name>
```

Release Information

Command introduced in Junos OS Release 8.2.

Description

On M320, M120, MX Series, PTX Series, T320, and T640 routers, clear Operation, Administration, and Management (OAM) link fault management statistics or state information from Ethernet interfaces.

Options

none—Clear OAM link fault management statistics from all Ethernet interfaces.

interface-name—(Optional) Clear OAM link fault management statistics from the specified Ethernet interface only.

Required Privilege Level

view

List of Sample Output

clear oam ethernet link-fault-management statistics on page 2833

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet link-fault-management statistics

```
user@host> clear oam ethernet link-fault-management statistics

Cleared link-fault-management statistics for all interfaces
```

CHAPTER 84

Operational Commands: Uplink Failure Detection

IN THIS CHAPTER

- show uplink-failure-detection | 2835

show uplink-failure-detection

Syntax

```
show uplink-failure-detection
<group  group-name>
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Display information about the uplink-failure-detection group, the member interfaces, and their status.

Options

none—Display information about all groups configured for uplink failure detection.

group *group-name*—(Optional) Display information about the specified group only.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) | 385

List of Sample Output

show uplink-failure-detection on page 2836

Output Fields

Table 256 on page 2835 lists the output fields for the **show uplink-failure-detection** command. Output fields are listed in the approximate order in which they appear.

Table 256: show uplink-failure-detection Output Fields

Field Name	Field Description
Group	Name of the group.
Uplink	The uplink interface or interfaces configured as link-to-monitor. **NOTE:** The asterisk (*) indicates that the link is up.

Table 256: show uplink-failure-detection Output Fields *(continued)*

Field Name	Field Description
Downlink	The downlink interface or interfaces configured as link-to-disable. **NOTE:** The asterisk (*) indicates that the link is up.
Failure Action	Status of uplink failure detection: • Active—The switch has detected an uplink failure and has brought the downlink down. • Inactive—The uplink or uplinks are up.

Sample Output

show uplink-failure-detection

```
user@switch> show uplink-failure-detection

Group              : group1
Uplink             :  ge-0/0/0*
Downlink           :  ge-0/0/1*
Failure Action     :  Inactive

Group              : group2
Uplink             :  ge-0/0/3.0
Downlink           :  ge-0/0/4.0
Failure Action     :  Active
```

CHAPTER 85

Operational Commands: RPM

IN THIS CHAPTER

- show services rpm active-servers | 2838
- show services rpm history-results | 2840
- show services rpm probe-results | 2845

show services rpm active-servers

Syntax

```
show services rpm active-servers
```

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 13.2 for PTX Series Packet Transport routers.
Command introduced in Junos OS Release 18.1 for QFX Series switches.

Description

Display the protocols and corresponding ports for which a router or switch is configured as a real-time performance monitoring (RPM) server.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show services rpm active-servers on page 2839

Output Fields

Table 217 on page 2594 lists the output fields for the **show services rpm active-servers** command. Output fields are listed in the approximate order in which they appear.

Table 257: show services rpm active-servers Output Fields

Field Name	Field Description
Protocol	Protocol configured on the receiving probe server. The protocol can be the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).
Port	Port configured on the receiving probe server.
Destination interface name	Output interface name for the probes.

Sample Output

show services rpm active-servers

```
user@host> show services rpm active-servers

    Protocol: TCP, Port: 50000, Destination interface name: lt-0/0/0.0
    Protocol: UDP, Port: 50001, Destination interface name: lt-0/0/0.0
```

show services rpm history-results

Syntax

```
show services rpm history-results
<brief | detail>
<dst-interface interface-name>
<owner owner>
<limit number>
<since time>
<source-address address>
<target-address address>
<test name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 on EX Series switches.
Command introduced in Junos OS Release 13.2 on PTX Series Packet Transport routers.
dst-interface, **limit**, **source-address**, and **target-address** options introduced in Junos OS Release 18.1R1 on MX Series.
owner and **test** options became optional in Junos OS Release 18.1R1 on MX Series.
Command introduced in Junos OS Release 18.1 on QFX Series switches.

Description

Display the results stored for the specified real-time performance monitoring (RPM) probes.

Options

none—(Optional) Display the results of the last 50 probes for all RPM instances.

brief | detail—(Optional) Display the specified level of output.

dst-interface *interface-name*—(Optional) Display information only for RPM probes that are generated on this MS-MPC or MS-MIC services interface. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

limit *number*—(Optional) Limit the number of results that are displayed. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

Range: 1 through 4,294,967,295

Default: 100

owner *owner*—(Optional) Display information only for probes with the specified probe owner. You must configure **owner** if you configure any of the following options: **dst-interface**, **limit**, **source-address**, or **target-address**.

since *time*—(Optional) Display information from the specified time. Specify time as ***yyyy-mm-dd.hh:mm:ss***.

source-address *address*—(Optional) Display information only for probes with the specified source address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

target-address *address*—(Optional) Display information only for probes with the specified target address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. You must also configure the **owner** option.

test *name*—(Optional starting in Junos OS Release 18.1R1) Display information only for the specified test.

Do not configure **test** if you configure any of the following options: **dst-interface**, **limit**, **source-address**, or **target-address**. These options do not work when you configure **test**.

Required Privilege Level
view

List of Sample Output
show services rpm history-results owner test on page 2842
show services rpm history-results owner test detail on page 2843

Output Fields
Table 218 on page 2597 lists the output fields for the **show services rpm history-results** command. Output fields are listed in the approximate order in which they appear.

Table 258: show services rpm history-results Output Fields

Field Name	Field Description	Level of Output
Owner	Probe owner.	All levels
Test	Name of a test for a probe instance.	All levels
Probe received	Timestamp when the probe result was determined.	All levels
Round trip time	Average ping round-trip time (RTT), in microseconds.	All levels
Probe results	Result of a particular probe performed by a remote host. The following information is contained in the results: • **Response received**—Timestamp when the probe result was determined. • **Rtt**—Average ping round-trip time (RTT), in microseconds.	**detail**

Table 258: show services rpm history-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over current test	Displays the results for the current test by probe at the time each probe was completed, as well as the status of the current test at the time the probe was completed.	**detail**
Probes sent	Number of probes sent with the current test.	**detail**
Probes received	Number of probe responses received within the current test.	**detail**
Loss percentage	Percentage of lost probes for the current test.	**detail**
Measurement	Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-pin-timestamp, the egress and ingress delay: • **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. • **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. • **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. • **Jitter**—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test. • **Stddev**—Standard deviation of the round-trip time, in microseconds, measured over the course of the current test.	**detail**

Sample Output

show services rpm history-results owner test

```
user@host> show services rpm history-results owner p1 test t1

     Owner, Test                 Probe received              Round trip time
    p1, t1                     Wed Aug 12 01:02:35 2009             315 usec
    p1, t1                     Wed Aug 12 01:02:36 2009             266 usec
    p1, t1                     Wed Aug 12 01:02:37 2009             314 usec
    p1, t1                     Wed Aug 12 01:02:38 2009             388 usec
```

```
p1, t1                      Wed Aug 12 01:02:39 2009             316 usec
p1, t1                      Wed Aug 12 01:02:40 2009             271 usec
p1, t1                      Wed Aug 12 01:02:41 2009             314 usec
p1, t1                      Wed Aug 12 01:02:42 2009            1180 usec
```

show services rpm history-results owner test detail

user@host> **show services rpm history-results owner p1 test t1 detail**

```
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:35 2009,
  Client and server hardware timestamps
  Rtt: 315 usec
Results over current test:
  Probes sent: 1, Probes received: 1, Loss percentage: 0
  Measurement: Round trip time
    Samples: 1, Minimum: 315 usec, Maximum: 315 usec, Average: 315 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 315 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:36 2009,
  Client and server hardware timestamps
  Rtt: 266 usec, Round trip jitter: -50 usec,
  Round trip interarrival jitter: 3 usec
Results over current test:
  Probes sent: 2, Probes received: 2, Loss percentage: 0
  Measurement: Round trip time
    Samples: 2, Minimum: 266 usec, Maximum: 315 usec, Average: 291 usec,
    Peak to peak: 49 usec, Stddev: 24 usec, Sum: 581 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:37 2009,
  Client and server hardware timestamps
  Rtt: 314 usec, Round trip jitter: 49 usec,
  Round trip interarrival jitter: 6 usec
Results over current test:
  Probes sent: 3, Probes received: 3, Loss percentage: 0
```

```
  Measurement: Round trip time
    Samples: 3, Minimum: 266 usec, Maximum: 315 usec, Average: 298 usec,
    Peak to peak: 49 usec, Stddev: 23 usec, Sum: 895 usec
  Measurement: Positive round trip jitter
    Samples: 1, Minimum: 49 usec, Maximum: 49 usec, Average: 49 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 49 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:38 2009,
  Client and server hardware timestamps
  Rtt: 388 usec, Round trip jitter: 74 usec,
  Round trip interarrival jitter: 10 usec
Results over current test:
  Probes sent: 4, Probes received: 4, Loss percentage: 0
  Measurement: Round trip time
    Samples: 4, Minimum: 266 usec, Maximum: 388 usec, Average: 321 usec,
    Peak to peak: 122 usec, Stddev: 44 usec, Sum: 1283 usec
  Measurement: Positive round trip jitter
    Samples: 2, Minimum: 49 usec, Maximum: 74 usec, Average: 62 usec,
    Peak to peak: 25 usec, Stddev: 12 usec, Sum: 123 usec
  Measurement: Negative round trip jitter
    Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec
```

show services rpm probe-results

Syntax

```
show services rpm probe-results
<dst-interface interface-name>
<limit number>
<owner owner>
<source-address address>
<status (fail | pass) >
<target-address address>
<terse>
<test name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 on EX Series switches.
Command introduced in Junos OS Release 13.2 on PTX Series Packet Transport Series routers.
dst-interface, **limit**, **source-address**, **status**, **target-address**, and **terse** options introduced in Junos OS Release 18.1R1 on MX Series.
Command introduced in Junos OS Release 18.1 on QFX Series switches.

Description

Display the results of the most recent real-time performance monitoring (RPM) probes.

Options

All the following options require that you also configure the **owner** option.

dst-interface *interface-name*—(Optional) Display information only for RPM probes that are configured on this MS-MPC or MS-MIC services interface. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

limit *number*—(Optional) Limit the number of results that are displayed. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

Range: 1 through 4,294,967,295

Default: 100

none—Display information for all of the most recent RPM probes.

owner *owner*—(Optional) Display information only for probes with the specified probe owner. You must configure **owner** if you configure any other options.

source-address *address*—(Optional) Display information only for probes with the specified source address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

status—(Optional) Display information only for probes with the specified type of test result. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface. Specify one of the following:

fail—Failed tests

pass—Passed tests

target-address *address*—(Optional) Display information only for probes with the specified target address. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

terse—(Optional) Display summary information. This option works only for RPM probes generated on an MS-MPC or MS-MIC services interface.

test *name*—(Optional) Display information only for the specified test.

Do not configure **test** if you configure any of the following options: **dst-interface**, **source-address**, or **target-address**. These options do not work when you configure **test**.

Required Privilege Level
view

List of Sample Output
show services rpm probe-results (IPv4 Targets) on page 2853
show services rpm probe-results (IPv6 Targets) on page 2856
show services rpm probe-results owner terse on page 2857
show services rpm probe-results owner status fail on page 2857
show services rpm probe-results (BGP Neighbor Discovery) on page 2857

Output Fields
Table 219 on page 2602 lists the output fields for the **show services rpm probe-results** command. Output fields are listed in the approximate order in which they appear.

Table 259: show services rpm probe-results Output Fields

Field Name	Field Description	Level of Output
Owner	Owner name. When you configure the probe owner statement at the **[edit services rpm]** hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-Bgp-Owner.**	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Test	Name of a test representing a collection of probes. When you configure the test test-name statement at the **[edit services rpm probe owner]** hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-BGP-Test-** *n*, where *n* is a cumulative number.	All levels
Target address	Destination IPv4 address used for the probes. This field is displayed when the probes are sent to the configured IPv4 or IPv6 targets or RPM servers.	none **dst-interface limit owner source-address target-address terse test**
Target inet6-address	Destination IPv6 address used for the probes. This field is displayed when the probes are sent to the configured IPv6 targets or RPM servers.	none **dst-interface limit owner source-address target-address terse test**
Source address	Source address used for the probes.	none **dst-interface limit owner source-address target-address test**
Probe type	Protocol configured on the receiving probe server: **http-get, http-metadata-get, icmp-ping, icmp-ping-timestamp, tcp-ping, udp-ping,** or **udp-ping-timestamp**.	none **dst-interface limit owner source-address target-address test**
Test size	Number of probes within a test.	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Routing Instance Name	(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured: • When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash **(/)** is used to separate the two entities. For example, if the routing instance called **R1** is configured within the logical system called **LS**, the name in the output field is **LS/R1**. • When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance. • When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by **default**. A slash (/) is used to separate the two entities. For example, **LS/default**.	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output

Probe results	Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:
	• **Response received**
	  ◦ **Probe sent time**—Timestamp when the probe's results was sent.
	  ◦ **Probe rcvd/timeout time**—Timestamp when the probe's results was received.
	• **Client and server hardware timestamps**—If timestamps are configured, an entry appears at this point.
	• **Rtt**—Average ping round-trip time (RTT), in microseconds.
	• **Egress jitter**—Egress jitter, in microseconds.
	• **Ingress jitter**—Ingress jitter, in microseconds.
	• **Round trip jitter**—Round-trip jitter, in microseconds.
	• **Egress interarrival jitter**—Egress interarrival jitter, in microseconds.
	• **Ingress interarrival jitter**—Ingress interarrival jitter, in microseconds.
	• **Round trip interarrival jitter**—Round-trip interarrival jitter, in microseconds.
		none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over current test	Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes. • **Probes sent**—Number of probes sent within the current test. • **Probes received**—Number of probe responses received within the current test. • **Loss percentage**—Percentage of lost probes for the current test. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over last test	Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed • **Probes sent**—Number of probes sent for the most recently completed test. • **Probes received**—Number of probe responses received for the most recently completed test. • **Loss percentage**—Percentage of lost probes for the most recently completed test. • **Test completed**—Time the most recent test was completed. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Results over all tests	Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test. • **Probes sent**—Number of probes sent in all tests. • **Probes received**—Number of probe responses received in all tests. • **Loss percentage**—Percentage of lost probes in all tests. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types **icmp-ping-timestamp** and **udp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.	none **dst-interface limit owner source-address target-address test**

Table 259: show services rpm probe-results Output Fields *(continued)*

Field Name	Field Description	Level of Output
Error Stats	Displays error statistics for each probe. • **Invalid client recv timestamp**—Number of client receive timestamp less than client send timestamp. • **Invalid server send timestamp**—Number of server send timestamp less than server receive timestamp. • **Invalid server processing time**—Number of server side spent time greater than RTT. NOTE: **Error Stats** is displayed in the output only if non-zero statistics exists.	none **dst-interface limit owner source-address target-address test**
Last Probe Status	Status of the last probe that was sent for the current test (**fail** or **pass**).	**status**
Status	Status of the last completed test (**up** or **down**).	**status terse**
Source-IF	The MS-MPC or MS-MIC services interface that generates the RPM probes.	**terse**

Sample Output

show services rpm probe-results (IPv4 Targets)

`user@host>` **show services rpm probe-results**

```
Owner: ADSN-J4300.ADSN-J2300.D2, Test: 75300002
Target address: 172.16.54.172, Source address: 10.206.0.1,
Probe type: udp-ping-timestamp, Test size: 10 probes
Probe results:
  Response received
  Probe sent time: Tue Feb  6 14:53:15 2007,
  Probe rcvd/timeout time: Tue Feb 6 14:53:15 2007
  Client and server hardware timestamps
  Rtt: 575 usec, Egress jitter: 5 usec, Ingress jitter: 8 usec,
  Round trip jitter: 12 usec, Egress interarrival jitter: 8 usec,
 Ingress interarrival jitter: 7 usec, Round trip interarrival jitter: 7 usec,

  Round trip interarrival jitter: 669 usec
```

```
Results over current test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec,  Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over last test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Test completed on Tue Feb  6 14:53:16 2007
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
```

```
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over all tests:
  Probes sent: 560, Probes received: 560, Loss percentage: 0
  Measurement: Round trip time
    Samples: 560, Minimum: 805 usec, Maximum: 3114 usec, Average: 1756 usec,
    Peak to peak: 2309 usec, Stddev: 519 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 257, Minimum: 0 usec, Maximum: 2054 usec, Average: 597 usec,
    Peak to peak: 2054 usec, Stddev: 427 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 302, Minimum: 1 usec, Maximum: 1812 usec, Average: 511 usec,
    Peak to peak: 1811 usec, Stddev: 408 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress  jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
```

```
   Error Stats:
       Invalid client recv timestamp: 3, Invalid server send timestamp: 0
       Invalid server processing time: 0
```

show services rpm probe-results (IPv6 Targets)

`user@host>` **show services rpm probe-results**

```
   Owner: p, Test: t1
   Target inet6-address: 2001:db8:0:1:2a0:a502:0:1da,
   Target Port : 34567 Test size: 1000000 probes
   Probe results:
     Response received
     Probe sent time: Mon Dec 16 10:48:07 2013
     Probe rcvd/timeout time: Mon Dec 16 10:48:07 2013
     Client and server hardware timestamps
     Rtt: 236 usec, Round trip jitter: -10 usec, Round trip interarrival jitter:
484 usec
   Results over current test:
     Probes sent: 10, Probes received: 10, Loss percentage: 0
     Measurement: Round trip time
      Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec, Peak
to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
     Measurement: Positive round trip jitter
       Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
     Measurement: Negative round trip jitter
       Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec
   Results over last test:
     Probes sent: 10, Probes received: 10, Loss percentage: 0
     Test completed on Mon Dec 16 10:48:07 2013
     Measurement: Round trip time
      Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec, Peak
to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
     Measurement: Positive round trip jitter
       Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
     Measurement: Negative round trip jitter
       Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec
   Results over all tests(From start of current control session):
     Probes sent: 490, Probes received: 488, Loss percentage: 0
     Measurement: Round trip time
```

```
        Samples: 488, Minimum: 231 usec, Maximum: 306 usec, Average: 270 usec,
Peak to peak: 75 usec, Stddev: 16 usec, Sum: 131586 usec
      Measurement: Positive round trip jitter
        Samples: 254, Minimum: 0 usec, Maximum: 10151 usec, Average: 157 usec,
Peak to peak: 10151 usec, Stddev: 873 usec, Sum: 39817 usec
      Measurement: Negative round trip jitter
        Samples: 233, Minimum: 1 usec, Maximum: 10170 usec, Average: 171 usec,
Peak to peak: 10169 usec, Stddev: 888 usec, Sum: 39889 usec
```

show services rpm probe-results owner terse

user@host> **show services rpm probe-results owner owner1 terse**

```
Test Name      Source-IF           Target Address      Status       Last Change
t_1            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S

t_2            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S

t_3            ms-2/2/0.10         192.0.2.1           UP           0D0H1M29S
```

show services rpm probe-results owner status fail

user@host> **show services rpm probe-results owner owner1 status fail**

```
Test Name              Last Probe Status         Status
t_1                    FAIL                      DOWN
t_2                    FAIL                      DOWN
t_3                    FAIL                      DOWN
```

show services rpm probe-results (BGP Neighbor Discovery)

user@host> **show services rpm probe-results**

```
Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
    Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
    Routing Instance Name: LS1/RI1
    Probe results:
      Response received
      Probe sent time: Fri Oct 28 05:20:23 2005
      Probe rcvd/timeout time: Fri Oct 28 05:20:23 2005
      Rtt: 662 usec
    Results over current test:
```

```
  Probes sent: 5, Probes received: 5, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
    Jitter: 133 usec, Stddev: 53 usec
Results over all tests:
  Probes sent: 5, Probes received: 5, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
    Jitter: 133 usec, Stddev: 53 usec
```

CHAPTER 86

Operational Commands: SNMP

IN THIS CHAPTER

- clear snmp statistics | **2860**
- request snmp spoof-trap | **2862**
- show snmp health-monitor | **2870**
- show snmp inform-statistics | **2879**
- show snmp mib | **2881**
- show snmp rmon | **2893**
- show snmp rmon history | **2899**
- show snmp statistics | **2904**
- show snmp v3 | **2912**

clear snmp statistics

Syntax

```
clear snmp 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 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Clear Simple Network Management Protocol (SNMP) statistics.

Options

This command has no options.

Required Privilege Level

clear

RELATED DOCUMENTATION

show snmp statistics | 2904

List of Sample Output

clear snmp statistics on page 2860

Output Fields

See **show snmp statistics** for an explanation of output fields.

Sample Output

clear snmp statistics

In the following example, SNMP statistics are displayed before and after the **clear snmp statistics** command is issued:

```
user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 8, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 8, Total set varbinds: 0,
    Get requests: 0, Get nexts: 8, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 2298, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 8, Traps: 2290
```

user@host> **clear snmp statistics**

```

```

user@host> **show snmp statistics**

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

request snmp spoof-trap

Syntax

```
request snmp spoof-trap
<trap> variable-bindings <object> <instance> <value>
```

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 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.

Options

<trap>—Name of the trap to spoof.

variable-bindings <*object*> <*instance*> <*value*>—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, **ifIndex[14] = 14**). Enclose the list of variable bindings in quotation marks (“ “) and use a comma to separate each object name, instance, and value definition (for example, **variable-bindings “ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2”**). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.

<dummy name>—A dummy trap name to display the list of available traps.

Question mark (?)—Question mark**?** to display possible completions.

Required Privilege Level

request

List of Sample Output

request snmp spoof-trap (with Variable Bindings) on page 2863
request snmp spoof-trap (Illegal Trap Name) on page 2863
request snmp spoof-trap (Question Mark ?) on page 2868

Sample Output

request snmp spoof-trap (with Variable Bindings)

`user@host>` **request snmp spoof-trap linkUp variable-bindings “ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2”**

```
Spoof trap request result: trap sent successfully
```

request snmp spoof-trap (Illegal Trap Name)

`user@host>` **request snmp spoof-trap xx**

```
Spoof trap request result: trap not found

Allowed Traps:
adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
  adslAtucPerfLolsThreshTrap
  adslAtucPerfLossThreshTrap
  adslAtucPerfLprsThreshTrap
  adslAtucRateChangeTrap
  adslAturPerfESsThreshTrap
  adslAturPerfLofsThreshTrap
  adslAturPerfLossThreshTrap
  adslAturPerfLprsThreshTrap
  adslAturRateChangeTrap
  apsEventChannelMismatch
  apsEventFEPLF
  apsEventModeMismatch
  apsEventPSBF
  apsEventSwitchover
  authenticationFailure
  bfdSessDown
  bfdSessUp
  bgpBackwardTransition
  bgpEstablished
  coldStart
  dlswTrapCircuitDown
  dlswTrapCircuitUp
  dlswTrapTConnDown
  dlswTrapTConnPartnerReject
  dlswTrapTConnProtViolation
```

```
dlswTrapTConnUp
dsx1LineStatusChange
dsx3LineStatusChange
entConfigChange
fallingAlarm
frDLCIStatusChange
ggsnTrapChanged
ggsnTrapCleared
ggsnTrapNew
gmplsTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisIDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAccessAuthServerDisabled
jnxAccessAuthServerEnabled
jnxAccessAuthServiceDown
jnxAccessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared
jnxCollFtpSwitchover
jnxCollMemoryAvailable
jnxCollMemoryUnavailable
jnxCollUnavailableDest
```

```
jnxCollUnavailableDestCleared
jnxCollUnsuccessfulTransfer
jnxDfcHardMemThresholdExceeded
jnxDfcHardMemUnderThreshold
jnxDfcHardPpsThresholdExceeded
jnxDfcHardPpsUnderThreshold
jnxDfcSoftMemThresholdExceeded
jnxDfcSoftMemUnderThreshold
jnxDfcSoftPpsThresholdExceeded
jnxDfcSoftPpsUnderThreshold
jnxEventTrap
jnxExampleStartup
jnxFEBSwitchover
jnxFanFailure
jnxFanOK
jnxFruCheck
jnxFruFailed
jnxFruInsertion
jnxFruOK
jnxFruOffline
jnxFruOnline
jnxFruPowerOff
jnxFruPowerOn
jnxFruRemoval
jnxHardDiskFailed
jnxHardDiskMissing
jnxJsAvPatternUpdateTrap
jnxJsChassisClusterSwitchover
jnxJsFwAuthCapacityExceeded
jnxJsFwAuthFailure
jnxJsFwAuthServiceDown
jnxJsFwAuthServiceUp
jnxJsNatAddrPoolThresholdStatus
jnxJsScreenAttack
jnxJsScreenCfgChange
jnxLdpLspDown
jnxLdpLspUp
jnxLdpSesDown
jnxLdpSesUp
jnxMIMstCistPortLoopProtectStateChangeTrap
jnxMIMstCistPortRootProtectStateChangeTrap
jnxMIMstErrTrap
jnxMIMstGenTrap
jnxMIMstInvalidBpduRxdTrap
```

```
jnxMIMstMstiPortLoopProtectStateChangeTrap
jnxMIMstMstiPortRootProtectStateChangeTrap
jnxMIMstNewRootTrap
jnxMIMstProtocolMigrationTrap
jnxMIMstRegionConfigChangeTrap
jnxMIMstTopologyChgTrap
jnxMacChangedNotification
jnxMplsLdpInitSesThresholdExceeded
jnxMplsLdpPathVectorLimitMismatch
jnxMplsLdpSessionDown
jnxMplsLdpSessionUp
jnxOspfv3IfConfigError
jnxOspfv3IfRxBadPacket
jnxOspfv3IfStateChange
jnxOspfv3LsdbApproachingOverflow
jnxOspfv3LsdbOverflow
jnxOspfv3NbrRestartHelperStatusChange
jnxOspfv3NbrStateChange
jnxOspfv3NssaTranslatorStatusChange
jnxOspfv3RestartStatusChange
jnxOspfv3VirtIfConfigError
jnxOspfv3VirtIfRxBadPacket
jnxOspfv3VirtIfStateChange
jnxOspfv3VirtNbrRestartHelperStatusChange
jnxOspfv3VirtNbrStateChange
jnxOtnAlarmCleared
jnxOtnAlarmSet
jnxOverTemperature
jnxPMonOverloadCleared
jnxPMonOverloadSet
jnxPingEgressJitterThresholdExceeded
jnxPingEgressStdDevThresholdExceeded
jnxPingEgressThresholdExceeded
jnxPingIngressJitterThresholdExceeded
jnxPingIngressStddevThresholdExceeded
jnxPingIngressThresholdExceeded
jnxPingRttJitterThresholdExceeded
jnxPingRttStdDevThresholdExceeded
jnxPingRttThresholdExceeded
jnxPortBpduErrorStatusChangeTrap
jnxPortLoopProtectStateChangeTrap
jnxPortRootProtectStateChangeTrap
jnxPowerSupplyFailure
jnxPowerSupplyOK
```

```
jnxRedundancySwitchover
jnxRmonAlarmGetFailure
jnxRmonGetOk
jnxSecAccessIfMacLimitExceeded
jnxSecAccessdsRateLimitCrossed
jnxSonetAlarmCleared
jnxSonetAlarmSet
jnxSpSvcSetCpuExceeded
jnxSpSvcSetCpuOk
jnxSpSvcSetZoneEntered
jnxSpSvcSetZoneExited
jnxStormEventNotification
jnxSyslogTrap
jnxTemperatureOK
jnxVccpPortDown
jnxVccpPortUp
jnxVpnIfDown
jnxVpnIfUp
jnxVpnPwDown
jnxVpnPwUp
jnxl2aldGlobalMacLimit
jnxl2aldInterfaceMacLimit
jnxl2aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange
mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp
mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecIllglLblThrshExcd
mplsTunnelDown
mplsTunnelReoptimized
mplsTunnelRerouted
mplsTunnelUp
```

```
mplsVrfIfDown
mplsVrfIfUp
mplsXCDown
mplsXCUp
msdpBackwardTransition
msdpEstablished
newRoot
ospfIfAuthFailure
ospfIfConfigError
ospfIfRxBadPacket
ospfIfStateChange
ospfLsdbApproachingOverflow
ospfLsdbOverflow
ospfMaxAgeLsa
ospfNbrStateChange
ospfOriginateLsa
ospfTxRetransmit
ospfVirtIfAuthFailure
ospfVirtIfConfigError
ospfVirtIfRxBadPacket
ospfVirtIfStateChange
ospfVirtIfTxRetransmit
ospfVirtNbrStateChange
pethMainPowerUsageOffNotification
pethMainPowerUsageOnNotification
pethPsePortOnOffNotification
pingProbeFailed
pingTestCompleted
pingTestFailed
ptopoConfigChange
risingAlarm
rpMauJabberTrap
sdlcLSStatusChange
sdlcPortStatusChange
topologyChange
traceRoutePathChange
traceRouteTestCompleted
traceRouteTestFailed
vrrpTrapAuthFailure
vrrpTrapNewMaster
warmStart
```

request snmp spoof-trap (Question Mark ?)

`user@host>` **request snmp spoof-trap ?**

```
Possible completions:
  <trap>               The name of the trap to spoof
  adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
  adslAtucPerfLolsThreshTrap
  adslAtucPerfLossThreshTrap
  adslAtucPerfLprsThreshTrap
  adslAtucRateChangeTrap
  adslAturPerfESsThreshTrap
  adslAturPerfLofsThreshTrap
  adslAturPerfLossThreshTrap
  adslAturPerfLprsThreshTrap
  adslAturRateChangeTrap
  apsEventChannelMismatch
  apsEventFEPLF
  apsEventModeMismatch
  apsEventPSBF
  apsEventSwitchover
  authenticationFailure
  bfdSessDown
  bfdSessUp
  bgpBackwardTransition
  bgpEstablished
  coldStart
  dlswTrapCircuitDown
  dlswTrapCircuitUp
---(more 10%)---
```

show snmp health-monitor

Syntax

```
show snmp health-monitor
<alarms <detail>> | <logs>
```

Release Information

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.

Options

none—Display information about all health monitor alarms and logs.

alarms <detail>—(Optional) Display detailed information about health monitor alarms.

logs—(Optional) Display information about health monitor logs.

Required Privilege Level

view

List of Sample Output

show snmp health-monitor on page 2872
show snmp health-monitor alarms detail on page 2875

Output Fields

Table 260 on page 2870 describes the output fields for the **show snmp health-monitor** command. Output fields are listed in the approximate order in which they appear.

Table 260: show snmp health-monitor Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
Variable description	Description of the health monitor object instance being monitored.	All levels
Variable name	Name of the health monitor object instance being monitored.	All levels
Value	Current value of the monitored variable in the most recent sample interval.	All levels

Table 260: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output

State	State of the alarm or event entry:
	• Alarms:
	  • **active**—Entry is fully configured and activated.
	  • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit.
	  • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit.
	  • **under creation**—Entry is being configured and is not yet activated.
	  • **startup**—Alarm is waiting for the first sample of the monitored variable.
	  • **object not available**—Monitored variable of that type is not available to the health monitor agent.
	  • **instance not available**—Monitored variable's instance is not available to the health monitor agent.
	  • **object type invalid**—Monitored variable is not a numeric value.
	  • **object processing errored**—An error occurred when the monitored variable was processed.
	  • **unknown**—State is not one of the above.
		All levels

Variable OID	Object ID to which the variable name is resolved. The format is **x.x.x.x**.	**detail**
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**.	**detail**

Table 260: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.
	• Alarm is *not* sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.
	  ◦ Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	**detail**
Creator	Mechanism by which the entry was configured (**Health Monitor**).	**detail**
Sample interval	Time period between samples (in seconds).	**detail**
Rising threshold	Upper limit threshold value as a percentage of the maximum possible value.	**detail**
Falling threshold	Lower limit threshold value as a percentage of the maximum possible value.	**detail**
Rising event index	Event triggered when the rising threshold is crossed.	**detail**
Falling event index	Event triggered when the falling threshold is crossed.	**detail**

Sample Output

show snmp health-monitor

```
user@host> show snmp health-monitor
```

```
Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                       58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                        0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                          0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                      35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                      0 active
       Chassis daemon                                  50 active
       Firewall daemon                                  0 active
       Interface daemon                                 5 active
       SNMP daemon                                     11 active
       MIB2 daemon                                     42 active
       Sonet APS daemon                                 0 active
       VRRP daemon                                      0 active
       Alarm daemon                                     3 active
       PFE daemon                                       0 active
       CRAFT daemon                                     0 active
       Traffic sampling control daemon                  0 active
       Ilmi daemon                                      0 active
       Remote operations daemon                         0 active
       CoS daemon                                       0 active
       Pic Services Logging daemon                      0 active
       Internal Routing Service Daemon                  3 active
       Network Access Service daemon                    0 active
       Forwarding UDP daemon                            0 active
       Routing socket proxy daemon                      0 active
       Disk Monitoring daemon                           1 active
       Inet daemon                                      0 active
       Syslog daemon                                    0 active
       Adaptive Services PIC daemon                     0 active
       ECC parity errors logging Daemon                 0 active
       Layer 2 Tunneling Protocol daemon                0 active
       PPPoE daemon                                     3 active
```

```
      Redundancy device daemon                              0 active
      PPP daemon                                            0 active
      Dynamic Flow Capture Daemon                           0 active

32776 Health Monitor: jroute daemon CPU utilization
      Routing protocol daemon                               1 active
      Management daemon                                     0 active
      Management daemon                                     0 active
      Command line interface                                4 active
      Periodic Packet Management daemon                     0 active
      Link Management daemon                                0 active
      Pragmatic General Multicast daemon                    0 active
      Bidirectional Forwarding Detection daemon             0 active
      SRC daemon                                            0 active
      audit daemon                                          0 active
      Event daemon                                          0 active

32777 Health Monitor: jcrypto daemon CPU utilization
      IPSec Key Management daemon                           0 active

32779 Health Monitor: jkernel daemon Memory utilization
      Init daemon                                       47384 active
      Chassis daemon                                    20204 active
      Firewall daemon                                    1956 active
      Interface daemon                                   3340 active
      SNMP daemon                                        4540 active
      MIB2 daemon                                        3880 active
      Sonet APS daemon                                   2632 active
      VRRP daemon                                        2672 active
      Alarm daemon                                       1856 active
      PFE daemon                                         2600 active
      CRAFT daemon                                       2000 active
      Traffic sampling control daemon                    3164 active
      Ilmi daemon                                        2132 active
      Remote operations daemon                           2964 active
      CoS daemon                                         3044 active
      Pic Services Logging daemon                        1944 active
      Internal Routing Service Daemon                    1392 active
      Network Access Service daemon                      1992 active
      Forwarding UDP daemon                              1876 active
      Routing socket proxy daemon                        1296 active
      Disk Monitoring daemon                             1180 active
      Inet daemon                                        1296 active
      Syslog daemon                                      1180 active
```

```
       Adaptive Services PIC daemon                    3220 active
       ECC parity errors logging Daemon                1100 active
       Layer 2 Tunneling Protocol daemon               3372 active
       PPPoE daemon                                    1424 active
       Redundancy device daemon                        1820 active
       PPP daemon                                      2060 active
       Dynamic Flow Capture Daemon                    10740 active
 32780 Health Monitor: jroute daemon Memory utilization
       Routing protocol daemon                         8104 active
       Management daemon                              13360 active
       Management daemon                              19252 active
       Command line interface                          9912 active
       Periodic Packet Management daemon               1484 active
       Link Management daemon                          2016 active
       Pragmatic General Multicast daemon              1968 active
       Bidirectional Forwarding Detection daemon       1956 active
       SRC daemon                                      1772 active
       audit daemon                                    1772 active
       Event daemon                                    1808 active

 32781 Health Monitor: jcrypto daemon Memory utilization
       IPSec Key Management daemon                     5600 active
```

show snmp health-monitor alarms detail

`user@host>` **show snmp health-monitor alarms detail**

```
Alarm Index 32768:
  Variable name                       jnxHrStoragePercentUsed.1
  Variable OID                        1.3.6.1.4.1.2636.3.31.1.1.1.1.1
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: root file system
                                      utilization
  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 58
    Instance State: active
```

```
Alarm Index 32769:
  Variable name                        jnxHrStoragePercentUsed.2
  Variable OID                         1.3.6.1.4.1.2636.3.31.1.1.1.1.2
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                                Health Monitor: /config file system
                                       utilization
  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold                  80
  Falling threshold                 70
  Rising event index              32768
  Falling event index             32768
    Instance Value: 0
    Instance State: active

Alarm Index 32770:
  Variable name                        jnxOperatingCPU.9.1.0.0
  Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                               Health Monitor: RE 0 CPU utilization


  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold                  80
  Falling threshold                 70
  Rising event index              32768
  Falling event index             32768
    Instance Value: 0
    Instance State: active

Alarm Index 32773:
  Variable name                        jnxOperatingBuffer.9.1.0.0
  Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                               Health Monitor: RE 0 Memory utilization
```

```
  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold                  80
  Falling threshold                 70
  Rising event index             32768
  Falling event index            32768
    Instance Value: 35
    Instance State: active

Alarm Index 32775:
  Variable name                        sysApplElmtRunCPU.3
  Variable OID                         1.3.6.1.2.1.54.1.2.3.1.9.3
  Sample type                          delta value
  Startup alarm                        rising alarm
  Owner                                Health Monitor: jkernel daemon CPU
                                       utilization
  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold               24000
  Falling threshold              21000
  Rising event index             32768
  Falling event index            32768
    Instance Name: sysApplElmtRunCPU.3.1.1
    Instance Description: Init daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.2.2786
    Instance Description: Chassis daemon
    Instance Value: 50
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.3.2938
    Instance Description: Firewall daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.4.2942
    Instance Description: Interface daemon
    Instance Value: 5
    Instance State: active
```

```
    Instance Name: sysApplElmtRunCPU.3.7.7332
    Instance Description: SNMP daemon
    Instance Value: 11
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.9.2914
    Instance Description: MIB2 daemon
    Instance Value: 42
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.12.2916
    Instance Description: Sonet APS daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.13.2917
    Instance Description: VRRP daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.14.2787
    Instance Description: Alarm daemon
    Instance Value: 3
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.15.2940
    Instance Description: PFE daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.16.2788
    Instance Description: CRAFT daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.17.2918
    Instance Description: Traffic sampling control daemon
---(more 23%)---
```

show snmp inform-statistics

Syntax

```
show snmp inform-statistics
```

Release Information

Command introduced in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) inform requests.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show snmp inform-statistics on page 2880

Output Fields

Table 261 on page 2879 describes the output fields for the **show snmp inform-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 261: show snmp inform-statistics Output Fields

Field Name	Field Description
Target Name	Name of the device configured to receive and respond to SNMP informs.
Address	IP address of the target device.
Sent	Number of informs sent to the target device and acknowledged by the target device.
Pending	Number of informs held in memory pending a response from the target device.
Discarded	Number of informs discarded after the specified number of retransmissions to the target device were attempted.
Timeouts	Number of informs that did not receive an acknowledgement from the target device within the timeout specified.

Table 261: show snmp inform-statistics Output Fields *(continued)*

Field Name	Field Description
Probe Failures	Connection failures that occurred (for example, when the target server returned invalid content or you incorrectly configured the target address).

Sample Output

show snmp inform-statistics

```
user@host> show snmp inform-statistics
```

```
Inform Request Statistics:
 Target Name: TA1_v3_md5_none Address: 172.17.20.184
  Sent: 176, Pending: 0
  Discarded: 0, Timeouts: 0, Probe Failures: 0
 Target Name: TA2_v3_sha_none Address: 192.168.110.59
  Sent: 0, Pending: 4
  Discarded: 84, Timeouts: 0, Probe Failures: 258
 Target Name: TA5_v2_none Address: 172.17.20.184
  Sent: 0, Pending: 0
  Discarded: 2, Timeouts: 10, Probe Failures: 0
```

show snmp mib

Syntax

```
show snmp mib (get | get-next | walk) (ascii | decimal | hex) object-id
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
ascii and **decimal** options introduced in Junos OS Release 9.6.
ascii and **decimal** options introduced in Junos OS Release 9.6 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
hex option introduced in Junos OS Release 19.2R2.
Behavior in regard to sysName.0 MIB object changed in Junos OS Release 19.1R1.

Description

Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.

> **NOTE:** Starting in Junos OS Release 18.3R1, SNMP queue statistics reporting for static interface-sets configured over Aggregate Ethernet (AE) interfaces is supported.
>
> Starting in Junos OS Release 19.1R1, the sysName.0 MIB object displays the fully qualified domain name. That is, if the hostname and domain name are configured on the system, both will show up for the sysName.0 MIB object.

Starting in Junos OS Release 20.2R1, We've introduced the new SNMP MIBs **jnxJsSPUMonitoringSPUThreadsNumber**, **jnxJsSPUMonitoringSPUThreadIndex**, **jnxJsSPUMonitoringSPUThreadLastMinUsage**, **jnxJsSPUMonitoringSPUThreadLastHourUsage**, and **jnxJsSPUMonitoringSPUThreadLastDayUsage** to monitor the CPU usage information of an SPC3 card.

Options

get—Retrieve and display one or more SNMP object values.

get-next—Retrieve and display the next SNMP object values.

walk—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.

NOTE: As of Junos OS Release 18.4R1, the CLI configuration command **set snmp customization ether-stats-ifd-only** is introduced. When **ether-stats-ifd-only** is configured, the **show snmp mib walk etherstatsTable** command displays data only for physical interfaces (IFDs). See customization (SNMP).

ascii—Display the SNMP object's string indices as an ASCII-key representation.

decimal—Display the SNMP object values in the decimal (default) format. The **decimal** option is the default option for this command. Therefore, issuing the **show snmp mib (get | get-next | walk) decimal object-id** and the **show snmp mib (get | get-next | walk) object-id** commands display the same output.

hex—Display the SNMP object values in the hexadecimal format.

object-id—The object can be represented by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). When entering multiple objects, enclose the objects in quotation marks.

Required Privilege Level

snmp—To view this statement in the configuration.

List of Sample Output

show snmp mib get on page 2883
show snmp mib get (Routing Engine) on page 2883
show snmp mib get (Routing Engine, PTX10003) on page 2883
show snmp mib get (Multiple Objects) on page 2884
show snmp mib get (Layer 2 Policer) on page 2884
show snmp mib get-next on page 2884
show snmp mib get-next (Specify an OID) on page 2884
show snmp mib walk on page 2884
show snmp mib walk (QFX Series) on page 2885
show snmp mib walk (ASCII) on page 2885
show snmp mib walk (Multiple Indices) on page 2885
show snmp mib walk decimal on page 2885
show snmp mib walk decimal (Multiple Indices) on page 2885
show snmp mib walk hex on page 2886
show snmp mib walk (Queue Statistics) on page 2886
show snmp mib walk bgp (MX Series) on page 2887
show snmp mib walk mplsL3VpnMIB (MX Series) on page 2888
show snmp mib walk (PTX10003) on page 2888
show snmp mib walk ascii jnxWlanWAPStatusTable (SRX320, SRX340, SRX345, and SRX550M) on page 2889
show snmp mib walk jnxWlanWAPClientTable (SRX320, SRX340, SRX345, and SRX550M) on page 2890

show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber (SRX5400, SRX5600, and SRX5800) on page 2890
show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex (SRX5400, SRX5600, and SRX5800) on page 2890
show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 (SRX5400, SRX5600, and SRX5800) on page 2891
show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 (SRX5400, SRX5600, SRX5800) on page 2891
show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 (SRX5400, SRX5600, and SRX5800) on page 2891

Output Fields

Table 262 on page 2883 describes the output fields for the **show snmp mib** command. Output fields are listed in the approximate order in which they appear.

Table 262: show snmp mib Output Fields

Field Name	Field Description
name	Object name and numeric instance value.
object value	Object value. The Junos OS translates OIDs into the corresponding object names.

Sample Output

show snmp mib get

```
user@host> show snmp mib get sysObjectID.0
```

```
sysObjectID.0 = jnxProductNameM20
```

show snmp mib get (Routing Engine)

```
user@router> show snmp mib get jnxFruName.9.1.0.0
```

```
jnxFruName.9.1.0.0 = Routing Engine 0
```

show snmp mib get (Routing Engine, PTX10003)

```
user@router> show snmp mib get jnxFruName.9.1.0.0
```

```
jnxFruName.9.1.0.0 = Routing Engine slot 0
```

show snmp mib get (Multiple Objects)

user@host> **show snmp mib get "sysObjectID.0 sysUpTime.0"**

```
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

show snmp mib get (Layer 2 Policer)

user@host> **show snmp mib get ifInOctets.25970**

```
ifInOctets.25970 = 7545720
```

show snmp mib get-next

user@host> **show snmp mib get-next jnxMibs**

```
jnxBoxClass.0 = jnxProductLineM20.0
```

show snmp mib get-next (Specify an OID)

user@host> **show snmp mib get-next 1.3.6.1**

```
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper
 Networks, Inc.
```

show snmp mib walk

user@host> **show snmp mib walk system**

```
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004
Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
sysContact.0 = Your contact
sysName.0 = my router
```

```
sysLocation.0 = building 1
sysServices.0 = 4
```

show snmp mib walk (QFX Series)

`user@switch>` **show snmp mib walk system**

```
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 138980301
sysContact.0  = System Contact
sysName.0     = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

show snmp mib walk (ASCII)

`user@host>` **show snmp mib walk ascii jnxUtilData**

```
jnxUtilCounter32Value."fred" = 100
```

show snmp mib walk (Multiple Indices)

`user@host>` **show snmp mib walk ascii jnxFWCounterByteCount**

```
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```

show snmp mib walk decimal

`user@host>`**show snmp mib walk decimal jnxUtilData**

```
jnxUtilCounter32Value.102.114.101.100 = 100
```

show snmp mib walk decimal (Multiple Indices)

`user@host>` **show snmp mib walk ascii jnxFWCounterByteCount**

```
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```

show snmp mib walk hex

`user@host>` **show snmp mib walk hex jnxBgpM2PeerRemoteAddr**

```
jnxBgpM2PeerRemoteAddr.0.1.10.0.3.3.1.10.0.3.1 = 0a 00 03 01
jnxBgpM2PeerRemoteAddr.0.1.32.32.32.9.1.32.32.32.32 = 00 00 00 00
jnxBgpM2PeerRemoteAddr.0.1.62.40.96.38.1.62.40.96.19 = 3e 28 60 13
jnxBgpM2PeerRemoteAddr.0.1.62.40.96.38.1.62.40.96.39 = 3e 28 60 27
```

show snmp mib walk (Queue Statistics)

To get interface-set queue statistics from jnxCosQstatQedPkts MIB with using interface-set SNMP index, use the following command:

`show snmp mib walk jnxCosQstatQedPkts.`*`interface-set snmp index`*

For example, if the interface-set SNMP index is 67108866

`user@host>` **show snmp mib walk jnxCosQstatQedPkts.67108866**

```
jnxCosQstatQedPkts.67108866.0 = 10
jnxCosQstatQedPkts.67108866.1 = 0
jnxCosQstatQedPkts.67108866.2 = 0
jnxCosQstatQedPkts.67108866.3 = 0
jnxCosQstatQedPkts.67108866.4 = 0
jnxCosQstatQedPkts.67108866.5 = 0
jnxCosQstatQedPkts.67108866.6 = 0
jnxCosQstatQedPkts.67108866.7 = 0
```

To get interface-set queue statistics from jnxCosIfsetQstatQedPkts MIB with using interface-set SNMP index, use the following command:

`show snmp mib walk jnxCosIfsetQstatQedPkts.`*`interface-set snmp index`*

For example, if the interface-set snmp index is 67108866

`user@host>` **show snmp mib walk jnxCosIfsetQstatQedPkts.67108866**

```
jnxCosIfsetQstatQedPkts.67108866.0 = 10
jnxCosIfsetQstatQedPkts.67108866.1 = 0
jnxCosIfsetQstatQedPkts.67108866.2 = 0
jnxCosIfsetQstatQedPkts.67108866.3 = 0
jnxCosIfsetQstatQedPkts.67108866.4 = 0
jnxCosIfsetQstatQedPkts.67108866.5 = 0
jnxCosIfsetQstatQedPkts.67108866.6 = 0
jnxCosIfsetQstatQedPkts.67108866.7 = 0
```

To get Interface-set queue statistics from jnxCosIfsetQstatQedPkts MIB using interface-set member IFL SNMP index, use the following command:

`show snmp mib walk jnxCosIfsetQstatQedPkts.`*`interface-set member IFL SNMP index`*

For example, if the interface-set member IFL SNMP is 519

`user@host>` **show snmp mib walk jnxCosIfsetQstatQedPkts.519**

```
jnxCosIfsetQstatQedPkts.519.0 = 10
jnxCosIfsetQstatQedPkts.519.1 = 0
jnxCosIfsetQstatQedPkts.519.2 = 0
jnxCosIfsetQstatQedPkts.519.3 = 0
jnxCosIfsetQstatQedPkts.519.4 = 0
jnxCosIfsetQstatQedPkts.519.5 = 0
jnxCosIfsetQstatQedPkts.519.6 = 0
jnxCosIfsetQstatQedPkts.519.7 = 0
```

show snmp mib walk bgp (MX Series)

Use the **show snmp mib walk bgp** to see the BGP versions.

`user@host>` **show snmp mib walk bgp**

```
bgpVersion.0  = 10
bgpLocalAs.0  = 1
bgpPeerIdentifier.2.2.2.2 = 2.2.2.2
bgpPeerIdentifier.3.3.3.3 = 3.3.3.3

bgpPeerInUpdates.2.2.2.2 = 3
bgpPeerInUpdates.3.3.3.3 = 2
bgpPeerOutUpdates.2.2.2.2 = 1
bgpPeerOutUpdates.3.3.3.3 = 1
bgpPeerInTotalMessages.2.2.2.2 = 11
```

```
bgpPeerInTotalMessages.3.3.3.3 = 10
bgpPeerOutTotalMessages.2.2.2.2 = 8
bgpPeerOutTotalMessages.3.3.3.3 = 8
```

show snmp mib walk mplsL3VpnMIB (MX Series)

Use the **show snmp mib walk mplsL3VpnMIB** to see attributes of L3VPN based MPLS.

`user@host>` **show snmp mib walk mplsL3VpnMIB**

```
mplsL3VpnConfiguredVrfs.0 = 1
mplsL3VpnActiveVrfs.0 = 1
mplsL3VpnConnectedInterfaces.0 = 1
mplsL3VpnNotificationEnable.0 = 2
mplsL3VpnVrfConfMaxPossRts.0 = 0
mplsL3VpnVrfConfRteMxThrshTime.0 = 0
mplsL3VpnIllLblRcvThrsh.0 = 0
mplsL3VpnIfVpnClassification.3.114.101.100.548 = 2
mplsL3VpnIfVpnRouteDistProtocol.3.114.101.100.548 = 40 7f
mplsL3VpnIfConfStorageType.3.114.101.100.548 = 5
mplsL3VpnIfConfRowStatus.3.114.101.100.548 = 1
mplsL3VpnVrfVpnId.3.114.101.100
mplsL3VpnVrfDescription.3.114.101.100 = red
mplsL3VpnVrfRD.3.114.101.100 = 2:1
mplsL3VpnVrfCreationTime.3.114.101.100 = 9111800
mplsL3VpnVrfOperStatus.3.114.101.100 = 1
mplsL3VpnVrfActiveInterfaces.3.114.101.100 = 1
mplsL3VpnVrfAssociatedInterfaces.3.114.101.100 = 1
mplsL3VpnVrfConfMidRteThresh.3.114.101.100 = 0
mplsL3VpnVrfConfHighRteThresh.3.114.101.100 = 0
mplsL3VpnVrfConfMaxRoutes.3.114.101.100 = 0
mplsL3VpnVrfConfLastChanged.3.114.101.100 = 9111800
```

show snmp mib walk (PTX10003)

On PTX10003-80C and PTX10003-160C devices, the **show snmp mib walk jnxFilledDescr** output shows only the fan tray number. This output does not show the number of fan slots present in each tray.

`user@router>` **show snmp mib walk jnxFilledDescr**

```
jnxFilledDescr.1.0.0.0 = Chassis
jnxFilledDescr.4.2.0.0 = Fan Tray 1
jnxFilledDescr.4.3.0.0 = Fan Tray 2
jnxFilledDescr.4.4.0.0 = Fan Tray 3
[...Output truncated...]
```

show snmp mib walk ascii jnxWlanWAPStatusTable (SRX320, SRX340, SRX345, and SRX550M)

Use the **show snmp mib walk ascii jnxWlanWAPStatusTable** command to monitor the Wi-Fi Mini-Physical Interface Module (Mini-PIM) status.

`user@host>` **show snmp mib walk ascii jnxWlanWAPStatusTable**

```
jnxWAPStatusIfdIndex.161 = 161
jnxWAPStatusIfdIndex.162 = 162
jnxWAPStatusAccessPoint.161 = bj345b_wl3_wap
jnxWAPStatusAccessPoint.162 = bj345b_wap
jnxWAPStatusType.161 = Internal
jnxWAPStatusType.162 = Internal
jnxWAPStatusLocation.161 = Default Location
jnxWAPStatusLocation.162 = Default Location
jnxWAPStatusSerialNumber.161
jnxWAPStatusSerialNumber.162
jnxWAPStatusFirmwareVersion.161 = v1.1.0
jnxWAPStatusFirmwareVersion.162 = v1.1.0
jnxWAPStatusAlternateVersion.161 = v1.1.0
jnxWAPStatusAlternateVersion.162 = v1.1.0
jnxWAPStatusCountry.161 = US
jnxWAPStatusCountry.162 = US
jnxWAPStatusAccessInterface.161 = wl-3/0/0
jnxWAPStatusAccessInterface.162 = wl-4/0/0
jnxWAPStatusSystemTime.161 = Fri Jun 21 05:05:42 UTC 2019
jnxWAPStatusSystemTime.162 = Fri Jun 21 05:38:46 UTC 2019
jnxWAPStatusPacketCapture.161 = Off
jnxWAPStatusPacketCapture.162 = Off
jnxWAPStatusEthernetPortMAC.161 = 56:48:0d:5e:8f:c5
jnxWAPStatusEthernetPortMAC.162 = 8a:b7:0a:7e:ad:8a
jnxWAPStatusEthernetIPv4.161
jnxWAPStatusEthernetIPv4.162
jnxWAPStatusRadio1Status.161 = On
jnxWAPStatusRadio1Status.162 = On
[...Output truncated...]
```

show snmp mib walk jnxWlanWAPClientTable (SRX320, SRX340, SRX345, and SRX550M)

Use the **show snmp mib walk jnxWlanWAPClientTable** command to monitor the Wi-Fi Mini-PIM client information.

`user@host>` **show snmp mib walk jnxWlanWAPClientTable**

```
jnxWAPClientIfdIndex.161.1 = 161
jnxWAPClientIfdIndex.162.1 = 162
jnxWAPClientIfdIndex.162.2 = 162
jnxWAPClientIndex.161.1 = 1
jnxWAPClientIndex.162.1 = 1
jnxWAPClientIndex.162.2 = 2
jnxWAPClientRadioID.161.1 = 1
jnxWAPClientRadioID.162.1 = 1
jnxWAPClientRadioID.162.2 = 1
jnxWAPClientSSID.161.1 = bj345b_wl3_5g
jnxWAPClientSSID.162.1 = bj345b_5g
jnxWAPClientSSID.162.2 = bj345b_5g
jnxWAPClientMAC.161.1 = e8:4e:06:64:38:89
jnxWAPClientMAC.162.1 = e8:4e:06:64:38:a3
jnxWAPClientMAC.162.2 = e8:4e:06:63:9d:f6
jnxWAPClientAuth.161.1 = NO
[...Output truncated...]
```

show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber** command to list the indices of flow threads in an SPU.

`user@host>` **show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber**

```
jnxJsSPUMonitoringSPUThreadsNumber.4 = 26
jnxJsSPUMonitoringSPUThreadsNumber.5 = 26
jnxJsSPUMonitoringSPUThreadsNumber.16 = 0
jnxJsSPUMonitoringSPUThreadsNumber.17 = 0
jnxJsSPUMonitoringSPUThreadsNumber.18 = 0
jnxJsSPUMonitoringSPUThreadsNumber.19 = 0
```

show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex** command to list the indices of flow threads in an SPU.

user@host> **show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex**

```
jnxJsSPUMonitoringSPUThreadIndex.4.0 = 0
jnxJsSPUMonitoringSPUThreadIndex.4.1 = 1
jnxJsSPUMonitoringSPUThreadIndex.4.2 = 2
jnxJsSPUMonitoringSPUThreadIndex.4.3 = 3

... ...

jnxJsSPUMonitoringSPUThreadIndex.5.22 = 22
jnxJsSPUMonitoringSPUThreadIndex.5.23 = 23
jnxJsSPUMonitoringSPUThreadIndex.5.24 = 24
jnxJsSPUMonitoringSPUThreadIndex.5.25 = 25
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8** command to monitor the average CPU usage for the last minute on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 = 0
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 (SRX5400, SRX5600, SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8** command to monitor the average CPU usage for the last hour on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 = 0
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8** command to monitor the average CPU usage for the last 24 hours on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 = 0
```

show snmp rmon

Syntax

```
show snmp rmon
<alarms <brief | detail> | events <brief | detail> | logs>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms, events, and logs.

Options

none—Display information about all RMON alarms and events.

alarms—(Optional) Display information about RMON alarms.

brief | detail—(Optional) Display brief or detailed information about RMON alarms or events.

events—(Optional) Display information about RMON events.

logs—(Optional) Display information about RMON monitoring logs.

Required Privilege Level

view

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Configuring RMON Alarms and Events | **652**
- Understanding RMON | **774**
- clear snmp statistics | **2860**
- clear snmp history | **2969**
- show snmp rmon history | **2899**

List of Sample Output

show snmp rmon on page 2896
show snmp rmon (QFX Series) on page 2896
show snmp rmon alarms detail on page 2897
show snmp rmon events detail on page 2897
show snmp rmon logs (QFX Series) on page 2898

Output Fields

Table 263 on page 2894 describes the output fields for the **show snmp rmon** command. Output fields are listed in the approximate order in which they appear.

Table 263: show snmp rmon Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
State	State of the alarm or event entry: Alarms: • **active**—Entry is fully configured and activated. • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit. • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit. • **under creation**—Entry is being configured and is not yet activated. • **startup**—Alarm is waiting for the first sample of the monitored variable. • **object not available**—Monitored variable of that type is not available to the SNMP agent. • **instance not available**—Monitored variable's instance is not available to the SNMP agent. • **object type invalid**—Monitored variable is not a numeric value. • **object processing errored**—An error occurred when the monitored variable was processed. • **unknown**—State is not one of the above. Events: • **active**—Entry has been fully configured and activated. • **under creation**—Entry is being configured and is not yet activated. • **unknown**—State is not one of the above.	All levels
Variable name	Name of the SNMP object instance being monitored.	All levels
Event Index	Event identifier.	All levels

Table 263: show snmp rmon Output Fields *(continued)*

Field Name	Field Description	Level of Output
Type	Type of notification made when an event is triggered. It can be one of the following: • **log**—A system log message is generated and an entry is made to the log table. • **snmptrap**—An SNMP trap is sent to the configured destination. • **log and trap**—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination. • **none**—Neither log nor trap will be sent.	**detail**
Last Event	Date and time of the last event. It has the format *yyyy-mm-dd hh:mm:ss timezone*.	**brief**
Community	Trap group used for sending the SNMP trap.	**detail**
Variable OID	Object ID to which the variable name is resolved. The format is **x.x.x.x**.	**detail**
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**.	**detail**

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.
	• Alarm is *not* sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.
	  ◦ Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	**detail**
Creator	Mechanism by which the entry was configured (**CLI** or **SNMP**).	**detail**

Table 263: show snmp rmon Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sample interval	Time period between samples (in seconds).	**detail**
Rising threshold	Upper limit threshold value configured by the user.	**detail**
Falling threshold	Lower limit threshold value configured by the user.	**detail**
Rising event index	Event triggered when the rising threshold is crossed.	**detail**
Falling event index	Event triggered when the falling threshold is crossed.	**detail**
Current value	Current value of the monitored variable in the most recent sample interval.	**detail**

Sample Output

show snmp rmon

```
user@host> show snmp rmon
```

```
Alarm
Index  State                       Variable name
    1  falling threshold crossed   ifInOctets.1

Event
Index  Type                        Last Event
    1  log and trap                2002-01-30 01:13:01 PST
```

show snmp rmon (QFX Series)

```
user@host> show snmp rmon
```

```
Alarm
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                          5 falling threshold
```

```
Event
Index  Type                          Last Event
    1  log and trap                  2009-07-10 11:34:17 PDT
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```

show snmp rmon alarms detail

user@host> **show snmp rmon alarms detail**

```
Alarm Index 1:
  Variable name                       ifInOctets.1
  Variable OID                        1.3.6.1.2.1.2.2.1.10.1
  Sample type                         delta value
  Startup alarm                       rising or falling alarm
  Owner                               monitor
  Creator                             CLI
  State                               falling threshold crossed
  Sample interval                  60 seconds
  Rising threshold             100000
  Falling threshold             80000
  Rising event index                1
  Falling event index               1
  Current value                     0
```

show snmp rmon events detail

user@host> **show snmp rmon events detail**

```
Event Index 1:
  Description                         rmon event
  Type                                log and trap
  Community                           rmon-trap-group
  Last event                          2009-07-10 11:34:17 PDT
  Creator                             CLI
  State                               active
```

show snmp rmon logs (QFX Series)

user@host> **show snmp rmon logs**

```
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```

show snmp rmon history

Syntax

```
show snmp rmon history
<history-index>
sample-index <sample-index>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display the contents of the RMON history group.

Options

none—Display all the entries in the RMON history group.

history-index—(Optional) Display the contents of the specified entry in the RMON history group.

sample-index *sample-index*—(Optional) Display the statistics collected for the specified sample within the specified entry in the RMON history group.

Required Privilege Level

view

RELATED DOCUMENTATION

- clear snmp history | **2969**
- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Configuring RMON Alarms and Events | **652**

List of Sample Output

show snmp rmon history 1 on page 2902
show snmp rmon history 1 sample-index 15 on page 2903

Output Fields

Table 264 on page 2900 lists the output fields for the **show smp rmon history** command. Output fields are listed in the approximate order in which they appear.

Table 264: show smp rmon history Output Fields

Field Name	Field Description
History Index	Identifies this RMON history entry within the RMON history group.
Owner	The entity that configured this entry. Range is 0 to 32 alphanumeric characters.
Status	The status of the RMON history entry.
Interface or **Data Source**	The ifndex object that identifies the interface that is being monitored.
Interval	The interval (in seconds) configured for this RMON history entry.
Buckets Requested	The requested number of buckets (**intervals**) configured for this RMON history entry.
Buckets Granted	The number of buckets granted for this RMON history entry.

Table 264: show smp rmon history Output Fields *(continued)*

Field Name	Field Description
Sample Index	The sample statistics taken at the specified interval. • **Drop Events**—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. • **Octets**—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. • **Packets**—Total number of packets. • **Broadcast Packets**—Number of broadcast packets. • **Multicast Packets**—Number of multicast packets. • **CRC 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). • **Undersize Pkts**—Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. • **Oversize Pkts**—Number of packets received during the sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets) but were otherwise well formed. • **Fragments**—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. • **Jabbers**—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. • **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. • **Utilization(%)**—The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Sample Output

show snmp rmon history 1

```
user@host> show snmp rmon history 1
```

```
 History Index 1:
 Interface                             171
 Requested Buckets                     50
 Interval                              10

Sample Index 1: Interval Start: Tue Feb 12 04:12:32 2008
    Drop Events         0
    Octets             486
    Packets             2
    Broadcast Packet    0
    Multicast Packets   2
    CRC errors          0
    Undersize Pkts      0
    Oversize Pkts       0
    Fragments           0
    Jabbers             0
    Collisions          0
    Utilization(%)      0

Sample Index 2: Interval Start: Tue Feb 12 04:12:42 2008
    Drop Events         0
    Octets             486
    Packets             2
    Broadcast Packet    0
    Multicast Packets   2
    CRC errors          0
    Undersize Pkts      0
    Oversize Pkts       0
    Fragments           0
    Jabbers             0
    Collisions          0
    Utilization(%)      0

Sample Index 3: Interval Start: Tue Feb 12 04:12:52 2008
    Drop Events         0
    Octets             486
    Packets             2
    Broadcast Packet    0
    Multicast Packets   2
```

```
    CRC errors          0
    Undersize Pkts      0
    Oversize Pkts       0
    Fragments           0
    Jabbers             0
    Collisions          0
    Utilization(%)      0
```

show snmp rmon history 1 sample-index 15

user@host> **show snmp rmon history 1 sample-index 15**

```
 Index 1
Owner    = monitor
Status    = valid
Data Source  = ifIndex.17
Interval   = 1800
Buckets Requested = 50
Buckets Granted = 50


Sample Index 44: Interval Start: Thu Jan  1 00:08:35 1970
Drop Events   = 0
Octetes   = 0
Packets   = 0
Broadcast Pkts  = 0
Multicast Pkts  = 0
CRC Errors  = 0
Undersize Pkts  = 0
Oversize Pkts  = 0
Fragments  = 0
Jabbers   = 0
Collisions  = 0
Utilization (%)  = 0
```

show snmp statistics

Syntax

```
show snmp statistics
<subagents>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Option **subagents** introduced in Junos OS Release 14.2.

Description

Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

Options

subagents—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

Required Privilege Level

view

RELATED DOCUMENTATION

clear snmp statistics | **2860**

List of Sample Output

show snmp statistics on page 2909
show snmp statistics subagents on page 2909

Output Fields

Table 265 on page 2905 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 265: show snmp statistics Output Fields

Field Name	Field Description
Input	Information about received packets: • **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service. • **Bad versions**—**(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. • **Bad community names**—**(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. • **Bad community uses**—**(snmpInBadCommunityUses)** Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. • **ASN parse errors**—**(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. • **Too bigs**—**(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**. • **No such names**—**(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values**—**(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**. • **Read onlys**—**(snmpInReadOnlys)** Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of **readOnly**. Only incorrect implementations of SNMP generate this error.

Table 265: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Input (continued)	• **General errors**—**(snmpInGenErrs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **genErr**. • **Total requests varbinds**—**(snmpInTotalReqVars)** Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP **GetRequest** and **GetNext** PDUs. • **Total set varbinds**—**(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs. • **Get requests**—**(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get nexts**—**(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity. • **Set requests**—**(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get responses**—**(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity. • **Traps**—**(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity. • **Silent drops**—**(snmpSilentDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • **Proxy drops**—**(snmpProxyDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration. • **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit.

Table 265: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
V3 Input	Information about SNMP version 3 packets: • **Unknown security models—(snmpUnknownSecurityModels)** Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • **Invalid messages—(snmpInvalidMsgs)** Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • **Unknown pdu handlers—(snmpUnknownPDUHandlers)** Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine. • **Unsupported security levels—(usmStatsUnsupportedSecLevels)** Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • **Not in time windows—(usmStatsNotInTimeWindows)** Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • **Unknown user names—(usmStatsUnknownUserNames)** Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • **Unknown engine ids—(usmStatsUnknownEngineIDs)** Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 265: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Output	Information about transmitted packets: • **Packets**—**(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service. • **Too bigs**—**(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**. • **No such names**—**(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values**—**(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**. • **General errors**—**(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**. • **Get requests**—**(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity. • **Get nexts**—**(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity. • **Set requests**—**(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity. • **Get responses**—**(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity. • **Traps**—**(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity.

Table 266 on page 2908 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 266: show snmp statistics subagents Output Fields

Field Name	Field Description
Subagent	Location of the SNMP subagent.
Request PDUs	Number of PDUs requested by the SNMP manager.
Response PDUs	Number of response PDUs sent by the SNMP subagent.
Request Variables	Number of variable bindings on the PDUs requested by the SNMP manager.
Response Variables	Number of variable bindings on the PDUs sent by the SNMP subagent.
Average Response Time	Average time taken by the SNMP subagent to send statistics response.

Table 266: show snmp statistics subagents Output Fields *(continued)*

Field Name	Field Description
Maximum Response Time	Maximum time taken by the SNMP subagent to send the statistics response.

Sample Output

show snmp statistics

```
user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12,
    Bad community uses: 0, ASN parse errors: 96,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 227084, Total set varbinds: 67,
    Get requests: 44942, Get nexts: 190371, Set requests: 10712,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0,
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 1
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
  Output:
    Packets: 246093, Too bigs: 0, No such names: 31561,
    Bad values: 0, General errors: 2,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 246025, Traps: 0
```

show snmp statistics subagents

```
user@host> show snmp statistics subagents

  Subagent: /var/run/cosd-20
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
```

```
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/pfed-30
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rmopd-15
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/chassisd-30
  Request PDUs: 33116, Response PDUs: 33116,
  Request Variables: 33116, Response Variables: 33116,
  Average Response Time(ms): 1.83,
  Maximum Response Time(ms): 203.48

Subagent: /var/run/pkid-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,
  Request Variables: 74211, Response Variables: 74211,
  Average Response Time(ms): 2.30,
  Maximum Response Time(ms): 51.04
```

```
Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
```

show snmp v3

Syntax

```
show snmp v3
<access <brief | detail> | community | general | groups | notify <filter> | target <address | parameters> | users>
```

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 Simple Network Management Protocol version 3 (SNMPv3) operating configuration.

Options

none—Display all of the SNMPv3 operating configuration.

access—(Optional) Display SNMPv3 access information.

brief | detail—(Optional) Display brief or detailed information about SNMPv3 access information.

community—(Optional) Display SNMPv3 community information.

general—(Optional) Display SNMPv3 general information.

groups—(Optional) Display SNMPv3 security-to-group information.

notify <filter>—(Optional) Display SNMPv3 notify and, optionally, notify filter information.

target <address | parameters>—(Optional) Display SNMPv3 target and, optionally, either target address or target parameter information.

users—(Optional) Display SNMPv3 user information.

Additional Information

To edit the default display of the **show snmp v3** command, specify options in the **show** statement at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

view

List of Sample Output

show snmp v3 on page 2914

Output Fields

Table 267 on page 2913 describes the output fields for the **show snmp v3** command. Output fields are listed in the approximate order in which they appear.

Table 267: show snmp v3 Output Fields

Field Name	Field Description
Access control	Information about access control: • **Group**—Group name for which the configured access privileges apply. The group, together with the context prefix and the security model and security level, forms the index for this table. • **Context prefix**—SNMPv3 context for which the configured access privileges apply. • **Security model/level**—Security model and security level for which the configuration access privileges apply. • **Read view**—Identifies the MIB view applied to SNMPv3 read operations. • **Write view**—Identifies the MIB view applied to SNMPv3 write operations. • **Notify view**—Identifies the MIB view applied to outbound SNMP notifications.
Engine	Information about local engine configuration: • **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • **Max msg size**—Maximum message size the sender can accommodate.
Engine ID	Information about engine ID: • **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • **Max msg size**—Maximum message size the sender can accommodate. • **Engine ID**—SNMPv3 engine ID associated with each user. • **User**—SNMPv3 user. • **Auth/Priv**—Authentication and encryption algorithm available for use by each user. • **Storage**—Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status. • **Status**—Status of the conceptual row. Only rows with an active status are used by the SNMPv3 engine.
Group name	Name of the group to which this entry belongs.

Table 267: show snmp v3 Output Fields *(continued)*

Field Name	Field Description
Security model	Identifies the security model context for the security name.
Security name	Used with the security model; identifies a specific security name instance. Each security model/security name combination can be assigned to a specific group.
Storage type	Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.
Status	Status of the conceptual row. Only rows with active status are used by the SNMPv3 engine.

Sample Output

show snmp v3

```
user@host> show snmp v3
```

```
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots:          38
Engine time:        64583 seconds
Max msg size:        2048 bytes

Engine ID: local
    User                            Auth/Priv   Storage      Status
    user1                            md5/des    nonvolatile  active
    user2                            sha/none   nonvolatile  active
    user3                           none/none   nonvolatile  active

Engine ID: 81 00 0a 4c 04 64 64 64 64
    User                            Auth/Priv   Storage      Status
    UNEW                             md5/none   nonvolatile  active
Group name           Security  Security             Storage      Status
                     model     name                 type
g1                   usm       user1                nonvolatile  active
g2                   usm       user2                nonvolatile  active
g3                   usm       user3                nonvolatile  active

Access control:
Group                Context Security      Read       Write     Notify
                     prefix  model/level   view       view      view
```

```
g1                          usm/privacy  v1         v1
g2                          usm/authent  v1         v1
g3                          usm/none     v1         v1
```

CHAPTER 87

Operational Commands: Port Mirroring

IN THIS CHAPTER

- show analyzer | **2917**

show analyzer

Syntax

```
show analyzer analyzer-name
```

Release Information

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

Description

Display information about analyzers configured for mirroring.

Options

analyzer-name—(Optional) Displays the status of a specific analyzer on the switch.

Required Privilege Level

view

List of Sample Output

show analyzer on page 2918

Output Fields

Table 220 on page 2616 lists the output fields for the **command-name** command. Output fields are listed in the approximate order in which they appear.

Table 268: show analyzer Output Fields

Field Name	Field Description
Analyzer name	Displays the name of the analyzer.
Output interface	Specifies a local interface to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Output VLAN	Specifies a VLAN to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Mirror ratio	Displays the ratio of packets to be mirrored.
Egress monitored interfaces	Displays interfaces for which traffic exiting the interfaces is mirrored.
Ingress monitored interfaces	Displays interfaces for which traffic entering the interfaces is mirrored.
Ingress monitored VLANs	Displays VLANs for which traffic entering the VLAN is mirrored.

Sample Output

show analyzer

user@host> **show analyzer**

```
Analyzer name           : employee-monitor
  Output interface             : ge-0/0/10.0
  Output VLAN                  : remote-analyzer
  Mirror ratio                 : 1
  Loss priority                : High
  Egress monitored interfaces  : ge-0/0/3.0
  Ingress monitored interfaces : ge-0/0/0.0
  Ingress monitored interfaces : ge-0/0/1.0
```

CHAPTER 88

Operational Commands: System Logging

IN THIS CHAPTER

- clear log | **2920**
- clear security log | **2922**
- clear security log file | **2924**
- clear security log stream file | **2925**
- monitor list | **2927**
- monitor start | **2929**
- monitor stop | **2931**
- request debug information | **2933**
- show log | **2936**
- show security log | **2944**
- show security log file | **2948**
- show security log severity | **2956**
- show security log query | **2957**

clear log

Syntax

```
clear log filename
<all>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Remove contents of a log file.

Options

filename—Name of the specific log file to delete. Note that the file name cannot contain any special characters, including: ![=;|(){}]

all—(Optional) Delete the specified log file and all archived versions of it.

Required Privilege Level

clear

RELATED DOCUMENTATION

show log | 2936

List of Sample Output

clear log on page 2920

Output Fields

See *file list* for an explanation of output fields.

Sample Output

clear log

The following sample commands list log file information, clear the contents of a log file, and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
```

```
lcc0-re0:
--------------------------------------------------------------------------
-rw-r-----  1 root  wheel      26450 Jun 23 18:47 /var/log/sampled
total 1
```

```
user@host> clear log lcc0-re0:sampled
```

```
lcc0-re0:
--------------------------------------------------------------------------
```

```
user@host> file list lcc0-re0:/var/log/sampled detail
```

```
lcc0-re0:
--------------------------------------------------------------------------
-rw-r-----  1 root  wheel         57 Sep 15 03:44 /var/log/sampled
total 1
```

clear security log

Syntax

```
clear security log
<all>
<all-logical-systems-tenants>
<destination-address>
<destination-port>
<event-id>
<failure>
<interface-name>
<newer-than>
<older--than>
<process>
<protocol>
<report>
<severity>
<source-address>
<source-port>
<success>
<username>
```

Release Information

Command introduced in Junos OS Release 11.2.
all-logical-systems-tenants option introduced in Junos OS Release 19.3R1.

Description

Delete the event log.

Options

all—Clear all audit event logs stored in the device memory.

all-logical-systems-tenants—Clear all audit event logs for all the logical systems and tenant systems.

destination-address—Clear audit event logs with the specified destination address.

destination-port—Clear audit event logs with the specified destination port.

event-id—Clear audit event logs with the specified event identification number.

failure—Clear failed audit event logs.

interface-name—Clear audit event logs with the specified interface.

newer-than—Clear audit event logs newer than the specified date and time.

older-than—Clear audit event logs older than the specified date and time

process—Clear audit event logs with the specified process that generated the event.

protocol—Clear audit event logs generated through the specified protocol.

report—Clear on-box reports for system traffic logs.

severity—Clear audit event logs generated with the specified severity.

source-address—Clear audit event logs with the specified source address.

source-port—Clear audit event logs with the specified source port.

success—Clear successful audit event logs.

username—Clear audit event logs generated for the specified user.

Required Privilege Level
clear

RELATED DOCUMENTATION

exclude (Security Log) | 2451
show security log | 2944

Sample Output

clear security log all

```
user@host> clear security log all
```

```
7905 security log events cleared
```

clear security log file

Syntax

```
clear security log file
```

Release Information
Command introduced in Junos OS Release 12.1.

Description
Deletes the content of an event mode security log file stored on the device in binary format.

Required Privilege Level
clear

RELATED DOCUMENTATION

show security log file | 2948

Sample Output

clear security log file

```
user@host> clear security log file
```

```
7905 security log events cleared
```

clear security log file logical-system LSYS1

```
user@host> clear security log file logical-system LSYS1
```

```
7905 security log events cleared
```

clear security log file tenant TSYS1

```
user@host> clear security log file tenant TSYS1
```

```
7905 security log events cleared
```

clear security log stream file

Syntax

```
clear security log query
clear security log stream
file <file-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D70 for SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances.

The **logical-system** and **tenant** options are introduced in Junos OS Release 19.2R1.

Description

- **clear security log query**—Clear the content of the database.
- **clear security log stream file**—Clear the content of the current log file.
- **clear security log stream file logical-system LSYS1** —Clear the content of the current log file for logical system.
- **clear security log stream file tenant TSYS1** —Clear the content of the current log file for tenant system.

Required Privilege Level

clear

Output Fields

The following outputs are occurred in two conditions:

- Clear log stream file successfully, when there is log file.
- Clear log stream file error or does not exits, when there is no log file.

Sample Output

clear security log stream file LSYS_f1.bin logical-system LSYS1

```
user@host> clear security log stream file LSYS_f1.bin logical-system LSYS1
```

```
Request to clear log stream file succeeds
```

clear security log stream file TSYS_f1.bin tenant-system TSYS1

```
user@host> clear security log stream file TSYS_f1.bin tenant-system TSYS1
```

```
Request to clear log stream file succeeds
```

monitor list

Syntax

```
monitor list
```

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 status of monitored log and trace files.

Options

This command has no options.

Additional Information

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are those configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

Required Privilege Level

trace

RELATED DOCUMENTATION

monitor start | 2929
monitor stop | 2931

List of Sample Output

monitor list on page 2928

Output Fields

Table 269 on page 2927 describes the output fields for the **monitor list** command. Output fields are listed in the approximate order in which they appear.

Table 269: monitor list Output Fields

Field Name	Field Description
monitor start	Indicates the file is being monitored.

Table 269: monitor list Output Fields *(continued)*

Field Name	Field Description
"*filename*"	Name of the file that is being monitored.
Last changed	Date and time at which the file was last modified.

Sample Output

monitor list

`user@host>` **monitor list**

```
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)
```

monitor start

Syntax

```
monitor start filename
```

Release Information

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

Description

Start displaying the system log or trace file and additional entries being added to those files.

Options

filename—Specific log or trace file.

Additional Information

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

> **NOTE:** To monitor a log file within a logical system, issue the **monitor start *logical-system-name/filename*** command.

Required Privilege Level

trace

RELATED DOCUMENTATION

monitor list | 2927
monitor stop | 2931

List of Sample Output

monitor start on page 2930

Output Fields

Table 270 on page 2930 describes the output fields for the **monitor start** command. Output fields are listed in the approximate order in which they appear.

Table 270: monitor start Output Fields

Field Name	Field Description
******filename******	Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.
Date and time	Timestamp for the log entry.

Sample Output

monitor start

```
user@host> monitor start system-log
```

```
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: RSA key generation complete.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: RSA authentication for root accepted.
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from host.example.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
```

monitor stop

Syntax

```
monitor stop filename
```

Release Information

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

Description

Stop displaying the system log or trace file.

Options

filename—Specific log or trace file.

Additional Information

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are those configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

Required Privilege Level

trace

RELATED DOCUMENTATION

monitor list | 2927
monitor start | 2929

List of Sample Output

monitor stop on page 2932

Output Fields

This command produces no output.

Sample Output

monitor stop

```
user@host> monitor stop
```

request debug information

Syntax

```
request debug information
<mgd>
```

Release Information

Command introduced in Junos OS Release 19.4R1 with **mgd** component.

Description

Consolidate debugging information for the component specified. You can issue the command without a component specified

Using this command speeds up the initial information-gathering phase of debugging. The output includes the combined output of multiple member commands.

Options

mgd—(Optional) Display debug information for the Mangement process (mgd) workflows.

Additional Information

The following commands are member commands executed by issuing the **request debug information mgd** command; the output of the **request debug information mgd** command consolidates the output of these member commands:

- show version no-forwarding
- show system uptime no-forwarding
- show system core-dumps no-forwarding
- show system storage no-forwarding
- show system processes extensive no-forwarding
- show mgd database-mappings
- show mgd database-mappings include-merge-view
- show mgd dop-refcount-statistics
- show mgd daemon-control-table
- show mgd database-statistics
- show mgd database-statistics committed
- show mgd ephemeral-instance-statistics
- show mgd expanded-configuration

- show mgd memory-statistics
- show system configuration database usage
- file list detail /var/rundb/
- file list detail /config/
- show system commit
- show system commit revision detail

> **NOTE:** Because the **request debug information** command executes various CLI commands that do not fit into one particular structure, the **request debug information | display xml** command will simply emit the output within a single set of output tags.

Required Privilege Level
view

List of Sample Output
request debug information mgd on page 2934

Sample Output

request debug information mgd

`user@host>` **request debug information mgd**

The following sample output gives only a subset of the output the command can display:

```
user@host> show system uptime no-forwarding

Current time: 2019-05-27 10:58:07 IST
Time Source:  LOCAL CLOCK
System booted: 2019-05-13 23:08:48 IST (1w6d 11:49 ago)
Protocols started: 2019-05-13 23:10:02 IST (1w6d 11:48 ago)
Last configured: 2019-05-27 10:29:52 IST (00:28:15 ago) by root
10:58AM  up 13 days, 11:49, 3 users, load averages: 0.66, 0.58, 0.60


user@host> show system core-dumps no-forwarding

/var/crash/*core*: No such file or directory
-rw-------  1 root  wheel    5909163 May 22 12:42 /var/tmp/mgd.core.0.gz
```

```
-rw-------  1 root  wheel    5997740 May 23 03:48 /var/tmp/mgd.core.1.gz
/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/var/jails/rest-api/tmp/*core*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
total files: 2


user@host> show mgd database-mappings


Database memory mappings information:

The schema database mapping address: 0xb99fe000
The configuration database mapping address: 0x90000000
The dbm maximum address: 0xbbbfe000
Is the extend-db feature enabled?  NO

Currently opened/mmapped databases:

Database file path                          Database mapped address         Current
 size        Maximum size   Database mapping flags
/var/run/db/schema.db                       0xb99fe000                      28672
KB            34816 KB       6


user@host> show mgd dop-refcount-statistics

Schema node name                Config object [name/value]       Parent object
name               reference-count   object-model      dop-pointer
parent-dop-pointer     is-junos-defaults?
————————————————————————————————————————————————————————————————————————————

juniper-config                  juniper-config                  NO PARENT (ROOT)
                2               SIMPLE            0x90104024
0x90104024             NO
version                         "20190520.071047_aahmad.r1018032 [aahmad]"
juniper-config         1                ATTRIB            0x912007a4
 0x90104024             NO
juniper-group                   juniper-group                   juniper-config
                 1              ORDCTN            0x90104124
0x90104024             NO
```

show log

List of Syntax

Syntax on page 2936
Syntax (QFX Series and OCX Series) on page 2936
Syntax (TX Matrix Router) on page 2936

Syntax

```
show log
<filename | user <username>>
```

Syntax (QFX Series and OCX Series)

```
show log filename
<device-type (device-id | device-alias)>
```

Syntax (TX Matrix Router)

```
show log
<all-lcc | lcc number | scc>
<filename | user <username>>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option *device-type (device-id | device-alias)* is introduced in Junos OS Release 13.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 20.3R1 for Next Gen Services on MX240, MX480, and MX960 routers.

Description

List log files, display log file contents, or display information about users who have logged in to the router or switch.

NOTE: On MX Series routers, modifying a configuration to replace a service interface with another service interface is treated as a catastrophic event. When you modify a configuration, the entire configuration associated with the service interface—including NAT pools, rules, and service sets—is deleted and then re-created for the newly specified service interface. If there are active sessions associated with the service interface that is being replaced, these sessions are deleted and the NAT pools are then released, which leads to the generation of the NAT_POOL_RELEASE system log messages. However, because NAT pools are already deleted as a result of the catastrophic configuration change and no longer exist, the NAT_POOL_RELEASE system log messages are not generated for the changed configuration.

Options

none—List all log files.

<all-lcc | lcc *number* | scc>—(Routing matrix only)(Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace ***number*** with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).

device-type—(QFabric system only) (Optional) Display log messages for only one of the following device types:

- **director-device**—Display logs for Director devices.
- **infrastructure-device**—Display logs for the logical components of the QFabric system infrastructure, including the diagnostic Routing Engine, fabric control Routing Engine, fabric manager Routing Engine, and the default network Node group and its backup (NW-NG-0 and NW-NG-0-backup).
- **interconnect-device**—Display logs for Interconnect devices.
- **node-device**—Display logs for Node devices.

NOTE: If you specify the **device-type** optional parameter, you must also specify either the **device-id** or **device-alias** optional parameter.

(*device-id* | *device-alias*)—If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).

filename—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.

NOTE: The *filename* parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of **messages**.

user <*username*>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include ***username***, display logging information about the specified user.

Required Privilege Level
trace

RELATED DOCUMENTATION

syslog (System) | **2510**

List of Sample Output

show log on page 2938
show log filename on page 2939
show log filename (QFabric System) on page 2941
show log user on page 2942
show log accepted-traffic (SRX4600, SRX5400, SRX5600, and SRX5800) on page 2942

Sample Output

show log

```
user@host> show log
```

```
total 57518
-rw-r--r--  1 root  bin      211663 Oct  1 19:44 dcd
-rw-r--r--  1 root  bin      999947 Oct  1 19:41 dcd.0
-rw-r--r--  1 root  bin      999994 Oct  1 17:48 dcd.1
-rw-r--r--  1 root  bin      238815 Oct  1 19:44 rpd
-rw-r--r--  1 root  bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r--  1 root  bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r--  1 root  bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r--  1 root  bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r--  1 root  bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r--  1 root  bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r--  1 root  bin     1056350 Sep 30 07:04 rpd.6
```

```
-rw-r--r--  1 root  bin     1048876 Sep 30 03:21 rpd.7
-rw-rw-r--  1 root  bin       19656 Oct  1 19:37 wtmp
```

show log filename

user@host> **show log rpd**

```
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct  1 18:00:18
Oct  1 18:00:19 KRT recv len 56 V9 seq 148 op add Type route/if af 2 addr 192.0.2.21
 nhop type local nhop 192.0.2.21
Oct  1 18:00:19 KRT recv len 56 V9 seq 149 op add Type route/if af 2 addr 192.0.2.22
 nhop type unicast nhop 192.0.2.22
Oct  1 18:00:19 KRT recv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct  1 18:00:19 KRT recv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct  1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...
```

user@host:LSYS1> **show log flow_lsys1.log**

```
Nov  7 07:34:09 07:34:09.491800:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table
lock

Nov  7 07:34:09 07:34:09.491809:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route
table lock

Nov  7 07:34:09 07:34:09.491840:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table
lock

Nov  7 07:34:09 07:34:09.491841:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route
table lock

Nov  7 07:34:09 07:34:09.491854:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh
 0x0

Nov  7 07:34:09 07:34:09.491868:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table
lock

Nov  7 07:34:09 07:34:09.491869:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route
```

```
table lock

Nov  7 07:34:09 07:34:09.491881:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh
 0x0
```

user@host:TSYS1> **show log flow_tsys1.log**

```
Nov  7 13:21:47
13:21:47.217744:CID-0:THREAD_ID-05:LSYS_ID-32:RT:<192.0.2.0/0->198.51.100.0/9011;1,0x0>
 :

Nov  7 13:21:47 13:21:47.217747:CID-0:THREAD_ID-05:LSYS_ID-32:RT:packet [84] ipid
 = 39281, @0x7f490ae56d52

Nov  7 13:21:47 13:21:47.217749:CID-0:THREAD_ID-05:LSYS_ID-32:RT:----
flow_process_pkt: (thd 5): flow_ctxt type 0, common flag 0x0, mbuf 0x4882b600,
rtbl7

Nov  7 13:21:47 13:21:47.217752:CID-0:THREAD_ID-05:LSYS_ID-32:RT: flow process pak
 fast ifl 88 in_ifp lt-0/0/0.101

Nov  7 13:21:47 13:21:47.217753:CID-0:THREAD_ID-05:LSYS_ID-32:RT:
lt-0/0/0.101:192.0.2.0->198.51.100.0, icmp, (0/0)

Nov  7 13:21:47 13:21:47.217756:CID-0:THREAD_ID-05:LSYS_ID-32:RT: find flow: table
 0x11d0a2680, hash 20069(0xffff), sa 192.0.2.0, da 198.51.100.0, sp 0, d0

Nov  7 13:21:47 13:21:47.217760:CID-0:THREAD_ID-05:LSYS_ID-32:RT:Found: session
id 0x12. sess tok 28685

Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow got session.


Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow session
id 18

Nov  7 13:21:47 13:21:47.217763:CID-0:THREAD_ID-05:LSYS_ID-32:RT: vector bits 0x200
 vector 0x84ae85f0

Nov  7 13:21:47 13:21:47.217764:CID-0:THREAD_ID-05:LSYS_ID-32:RT:set nat
0x11e463550(18) timeout const to 2

Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT: set_nat_timeout
 2 on session 18
```

```
Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT:refresh nat
0x11e463550(18) timeout to 2

Nov  7 13:21:47 13:21:47.217767:CID-0:THREAD_ID-05:LSYS_ID-32:RT:insert usp tag
for apps

Nov  7 13:21:47 13:21:47.217768:CID-0:THREAD_ID-05:LSYS_ID-32:RT:mbuf 0x4882b600,
 exit nh 0xfffb0006
```

show log filename (QFabric System)

`user@qfabric>` **show log messages**

```
Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242726)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 242757)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486 file:
 UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486 file:
 UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
```

```
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492 file:
 UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492 file:
 UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)
```

show log user

user@host> **show log user**

```
usera    mg2546                  Thu Oct  1 19:37   still logged in
usera    mg2529                  Thu Oct  1 19:08 - 19:36  (00:28)
usera    mg2518                  Thu Oct  1 18:53 - 18:58  (00:04)
root     mg1575                  Wed Sep 30 18:39 - 18:41  (00:02)
root     ttyp2    aaa.bbbb.com   Wed Sep 30 18:39 - 18:41  (00:02)
userb    ttyp1    192.0.2.0      Wed Sep 30 01:03 - 01:22  (00:19)
```

show log accepted-traffic (SRX4600, SRX5400, SRX5600, and SRX5800)

user@host> **show log accepted-traffic**

```
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
3.3.3.5/2->4.4.4.2/63 0x0 None 3.3.3.5/2->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2617282058 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
3.3.3.4/4->4.4.4.2/63 0x0 None 3.3.3.4/4->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2550162754 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
3.3.3.4/1->4.4.4.2/63 0x0 None 3.3.3.4/1->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2550162755 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
3.3.3.3/0->4.4.4.2/63 0x0 None 3.3.3.3/0->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2550162752 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
```

```
3.3.3.5/5->4.4.4.2/63 0x0 None 3.3.3.5/5->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2550162751 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
Jul 17 20:26:04  sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created
3.3.3.3/3->4.4.4.2/63 0x0 None 3.3.3.3/3->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2
TRUST UNTRUST 2550162753 N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
N/A N/A N/A
```

show security log

Syntax

```
show security log {all| destination-address| destination-port| event-id| failure|interface-name| newer-than| older-than|
    process| protocol|report| severity| sort-by| source-address| source-port| success| user}
```

Release Information
Command introduced in Junos OS Release 11.2 .

Description
Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.

Options
all—Display all audit event logs stored in the device memory.

destination-address—Display audit event logs with the specified destination address.

destination-port—Display audit event logs with the specified destination port.

event-id—Display audit event logs with the specified event identification number.

failure—Display failed audit event logs.

interface-name—Display audit event logs with the specified interface.

newer-than—Display audit event logs newer than the specified date and time.

older-than—Display audit event logs older than the specified date and time.

process—Display audit event logs with the specified process that generated the event.

protocol—Display audit event logs generated through the specified protocol.

report—Display on-box reports for system traffic logs.

severity—Display audit event logs generated with the specified severity.

sort-by—Display audit event logs generated sorted with the specified options.

source-address—Display audit event logs with the specified source address.

source-port—Display audit event logs with the specified source port.

success—Display successful audit event logs.

username—Display audit event logs generated for the specified user.

Required Privilege Level
view

RELATED DOCUMENTATION

exclude (Security Log) | 2451
clear security log | 2922

List of Sample Output
show security log on page 2945

Output Fields
Table 271 on page 2945 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

Table 271: show security log Output Fields

Field Name	Field Description
Event time	The timestamp of the events received. Security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs.
Message	Security events are listed.

Sample Output

show security log

```
user@host> show security log
```

```
Event time               Message
2010-10-22 13:28:37 CST  session created 1.1.1.2/1-->2.2.2.2/1308
 icmp 1.1.1.2/1-->2.2.2.2/1308
 None None 1 policy1 trustZone untrustZone 52 N/A(N/A) ge-0/0/1.0
2010-10-22 13:28:38 CST  session created 1.1.1.2/1-->2.2.2.2/1308 icmp
1.1.1.2/1-->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0
```

```
...
```

```
2010-10-22 13:36:12 CST  session denied m icmp 1(8) policy1 trustZone untrustZone
 N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST  session denied 1.1.1.2/2-->2.2.2.2/54812  icmp 1(8) policy1
 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...
```

```
2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST  IP spoofing! source: source: 2.2.2.20, destination:
2.2.2.2, protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action:
 drop

...
```

```
2011-02-18 15:53:34 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/crl/ca-profile1.crl
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

...
```

```
2011-03-14 23:00:40 PDT  IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
```

```
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]

...
```

```
Event time               Message
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 .5 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
 log '
```

show security log file

Syntax

```
show security log file
```

Release Information
Command introduced in Junos OS Release 12.1.

Description
Enables customers to view event-mode log files stored on the device in binary format.

Required Privilege Level
view

RELATED DOCUMENTATION

show security log | 2944

List of Sample Output
show security log file on page 2948

Output Fields
Table 272 on page 2948 lists the output fields for the **show security log file** command. Output fields are listed in the approximate order in which they appear.

Table 272: show security log file Output Fields

Field Name	Field Description
Event time	The timestamp when the security event was received.
Message	The message describing the security event.

Sample Output

show security log file

```
user@host> show security log file
```

```
<14>1 2011-08-28T21:14:43 topstar RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.34 source-address="7.7.7.2" source-port="1"
destination-address="8.8.8.2" destination-port="5636" service-name="icmp"
nat-source-address="7.7.7.2" nat-source-port="1" nat-destination-address="8.8.8.2"
 nat-destination-port="5636" src-nat-rule-name="None" dst-nat-rule-name="None"
protocol-id="1" policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000442" username="N/A" roles="N/A"
 packet-incoming-interface="ge-0/0/0.0"]

<14>1 2011-08-28T21:14:45 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="7.7.7.2"
source-port="0" destination-address="8.8.8.2" destination-port="5636"
service-name="icmp" nat-source-address="7.7.7.2" nat-source-port="0"
nat-destination-address="8.8.8.2" nat-destination-port="5636"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="1"
policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000441" packets-from-client="1"
bytes-from-client="84" packets-from-server="1" bytes-from-server="84"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/0.0"]

...
```

user@host> **show security log file**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
```

```
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

user@host>**show security log file bin_msg**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]
```

```
<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

user@host>**show security log file bin_msg logical-system LSYS1**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
```

```
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

user@host>**show security log file bin_msg tenant TSYS1**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
```

```
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

user@host>**show security log stream file s1_f1**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]
```

```
 ...
```

user@host>**show security log stream file s1_f1 logical-system LSYS1**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

user@host>**show security log stream file s1_f1 tenant TSYS1**

```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" packets-from-client="1"
 bytes-from-client="104" packets-from-server="1" bytes-from-server="104"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

show security log severity

Syntax

```
show security log severity
```

Release Information

Command introduced in Junos OS Release 15.1X49-D40.

Description

Display severity information for the event.

Required Privilege Level

view

RELATED DOCUMENTATION

show security log | 2944

Output Fields

Table 272 on page 2948 lists the output fields for the **show security log severity** command. Output fields are listed in the approximate order in which they appear.

Table 273: show security log severity Output Fields

Field Name	Field Description
alert	**Alert severity**
crit	**Critical severity**
debug	**Debug severity**
emerg	**Emergency severity**
err	**Error severity**
info	**Information severity**
notice	**Notice severity**
warning	**Warning severity**

show security log query

List of Syntax

Show Security Log Query on page 2957
Show Security Log Stream on page 2957

Show Security Log Query

```
show security log query {category all | utm | idp | alg | appqos | flow | fw-auth | gtp | ipsec | nat | pst-ds-lite | rtlog | screen
  | sctp | secintel} count < count>
[src-ip <src-ip>]
[dst-ip <dst-ip>]
[src-port <src-port>]
[dst-port <dst-port>]
[application <application>]
[user <user>]
[event-type <event-type>]
[service <service>]
[start-time <start-time>]
[stop-time <stop-time>]
```

Show Security Log Stream

```
show security log stream
file <filename>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D70 for SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances.

Description

- **show security log query**—View the security log from the database with query conditions.
- **show security log stream file**—View all the security log messages in the specified log file. Use the **/var/log/hostlogs** directory to search the specified log file, and use the **show security log stream file** command to view logs in log files in the **/var/log/hostlogs** directory.

Options

- count—The log number to output.
- scr-ip—The source IP address of log messages.
- dst-ip—The destination IP address of log messages.
- src-port—The source port of log messages.

- dst-port—The destination port of log messages.
- application—The application of log messages.
- user—The user of log messages.
- event-type—The event type of log messages.
- service—The service of log messages.
- start-time—The earliest timestamp of log messages; the format for time is YYYY-MM-DDTHH:MM:SS.
- stop-time—The latest timestamp of log messages.

Required Privilege Level
view

RELATED DOCUMENTATION

clear security log query

clear security log stream file

List of Sample Output
show security log query on page 2958
show security log stream file <file-name> on page 2959

Sample Output

show security log query

`rootr@dut>` **show security log query category flow count 20 src-ip 211.0.0.2 start-time 2013-11-29T00:00:00 end-time 2013-11-29T23:59:00**

```
<14>1 2013-11-29T16:01:26.820+08:00 plat02 RT_FLOW - RT_FLOW_SESSION_CLOSE
reason="CLI" source-address="211.0.0.2" source-port="20263"
destination-address="211.0.1.3" destination-port="4903" service-name="None"
nat-source-address="30.0.11.11" nat-source-port="27140"
nat-destination-address="211.0.1.3" nat-destination-port="4903"
src-nat-rule-name="src_rs2_rule1" dst-nat-rule-name="None" protocol-id="17"
policy-name="p1" source-zone-name="green" destination-zone-name="red"
session-id-32="30" packets-from-client="1" bytes-from-client="60"
packets-from-server="0" bytes-from-server="0" elapsed-time="92683"
application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/1.0" encrypted="UNKNOWN"
```

show security log stream file <file-name>

```
root@dut> show security log stream file traffic.log
```

```
<14>1 2013-11-29T16:01:26.820+08:00 plat02 RT_FLOW - RT_FLOW_SESSION_CLOSE
reason="CLI" source-address="211.0.0.2" source-port="20263"
destination-address="211.0.1.3" destination-port="4903" service-name="None"
nat-source-address="30.0.11.11" nat-source-port="27140"
nat-destination-address="211.0.1.3" nat-destination-port="4903"
src-nat-rule-name="src_rs2_rule1" dst-nat-rule-name="None" protocol-id="17"
policy-name="p1" source-zone-name="green" destination-zone-name="red"
session-id-32="30" packets-from-client="1" bytes-from-client="60"
packets-from-server="0" bytes-from-server="0" elapsed-time="92683"
application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/1.0" encrypted="UNKNOWN"] session closed CLI:
211.0.0.2/20263->211.0.1.3/4903 None 30.0.11.11/27140->211.0.1.3/4903 src_rs2_rule1
 None 17 p1 green red 30 1(60) 0(0) 92683 UNKNOWN UNKNOWN N/A(N/A) ge-0/0/1.0
UNKNOWN
```

CHAPTER 89

Monitoring Operational Commands

IN THIS CHAPTER

- clear chassis cluster ip-monitoring failure-count | **2962**
- clear chassis cluster ip-monitoring failure-count ip-address | **2963**
- clear ilmi statistics | **2965**
- clear interfaces statistics | **2966**
- clear services rpm twamp server connection | **2968**
- clear snmp history | **2969**
- clear snmp statistics | **2970**
- request packet-capture start | **2972**
- request packet-capture stop | **2978**
- request pppoe connect | **2979**
- request pppoe disconnect | **2980**
- request services ip-monitoring preempt-restore policy | **2981**
- request services rpm twamp start | **2983**
- request services rpm twamp stop | **2984**
- request snmp spoof-trap | **2985**
- request snmp utility-mib set instance | **2993**
- request snmp utility-mib clear instance | **2994**
- request support information | **2995**
- show chassis alarms | **3013**
- show chassis cluster ip-monitoring status redundancy-group | **3015**
- show interfaces snmp-index | **3019**
- show interfaces summary | **3021**
- show ilmi statistics | **3023**
- show security alarms | **3028**
- show security datapath-debug capture | **3034**
- show security datapath-debug counter | **3036**
- show security monitoring | **3038**
- show security monitoring fpc fpc-number | **3041**

- show security monitoring performance session | 3045
- show security monitoring performance spu | 3047
- show services ip-monitoring status | 3051
- show services rpm twamp client connection | 3056
- show services rpm twamp client history-results | 3058
- show services rpm twamp client probe-results | 3061
- show services rpm twamp client session | 3068
- show services rpm twamp server connection | 3070
- show services rpm twamp server session | 3072
- show snmp health-monitor | 3074
- show snmp inform-statistics | 3083
- show snmp mib | 3085
- show snmp rmon | 3097
- show snmp statistics | 3103
- show snmp stats-response-statistics | 3111
- show snmp v3 | 3114
- show system alarms | 3118
- show system alarms | 3119
- show system khms-stats | 3124
- show system monitor memory events | 3131
- show system monitor memory status | 3134
- show system monitor memory actions | 3137
- show system resource-monitor fpc | 3139

clear chassis cluster ip-monitoring failure-count

Syntax

```
clear chassis cluster ip-monitoring failure-count
```

Release Information

Command introduced in Junos OS Release 10.1.

Description

Clear the failure count for all IP addresses.

Required Privilege Level

clear

RELATED DOCUMENTATION

clear chassis cluster ip-monitoring failure-count ip-address | 2963

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count
```

```
node0:
--------------------------------------------------------------------------
Cleared failure count for all IPs

node1:
--------------------------------------------------------------------------
Cleared failure count for all IPs
```

clear chassis cluster ip-monitoring failure-count ip-address

Syntax

```
clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1
```

Release Information

Command introduced in Junos OS Release 10.1.

Description

Clear the failure count for a specified IP address.

> **NOTE:** Entering an IP address at the end of this command is optional. If you do not specify an IP address, the failure count for all monitored IP addresses is cleared.

Required Privilege Level

clear

RELATED DOCUMENTATION

clear chassis cluster failover-count

clear chassis cluster ip-monitoring failure-count | 2962

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1
```

```
node0:
--------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1

node1:
```

```
--------------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1
```

clear ilmi statistics

Syntax

```
clear ilmi statistics
```

Release Information
Command introduced before Junos OS Release 7.4.

Description
Set Integrated Local Management Interface (ILMI) statistics to zero.

Options
This command has no options.

Required Privilege Level
clear

RELATED DOCUMENTATION

show ilmi statistics | 3023

List of Sample Output
clear ilmi statistics on page 2965

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ilmi statistics

```
user@host> clear ilmi statistics
```

clear interfaces statistics

Syntax

```
clear interfaces statistics (all | interface-name)
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 19.2R1 for QSFP-100GE-DWDM2 transceiver on MX10003, MX10008, MX10016, and MX204 routers.

Description

Set interface statistics to zero. If you issue the **clear interfaces statistics *interface-name*** command and then perform a graceful Routing Engine switchover, the interface statistics are not cleared on the new master. Reissue the command to clear the interface statistics again.

Starting in Junos OS Release 17.3R1, this command supports the clearing of Packet Forwarding Engine accounting statistics on logical interfaces configured with accounting options. On these interfaces, the current statistics values are stored as the new current baseline values and then the counters are reset to zero. If the **allow-clear** statement is included in the interface profile, then the cleared statistics values are reported to the accounting options flat file associated with the interface. Reporting is disabled by default; if **allow-clear** is not configured, then the CLI displays cleared statistics counters, but they are not reported to the flat file.

Starting in Junos OS Release 19.1R1, this command supports the clearing of unicast Reverse Path Forwarding (RPF) statistics.

Options

all—Set statistics on all interfaces to zero.

interface-name—Set statistics on a particular interface to zero.

Required Privilege Level

clear

List of Sample Output

clear interfaces statistics on page 2967

Output Fields

When you enter this command, you are provided no feedback on the status of your request.

Sample Output

clear interfaces statistics

```
user@host> clear interfaces statistics
```

clear services rpm twamp server connection

Syntax

clear services rpm twamp server connection
<connection-id>

Release Information

Command introduced in Junos OS Release 15.1 for SRX Series devices.

Description

Clear connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default all established connections are cleared (along with the sessions on those connections). To clear only a specific connection, specify the connection ID when you issue the command.

Options

connection-id—(Optional) Clears specific connection as per the ID mentioned.

Required Privilege Level

clear

clear snmp history

Syntax

```
clear snmp history (index | all)
```

Release Information

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

Description

Delete the history record of collected samples of SNMP Ethernet statistics.

Options

all—Clear all the entries in the history index.

index—Clear the contents of the specified entry in the history index.

Required Privilege Level

clear

RELATED DOCUMENTATION

clear snmp statistics | **2860**

Configuring RMON History Sampling | **791**

clear snmp statistics

Syntax

```
clear snmp 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 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Clear Simple Network Management Protocol (SNMP) statistics.

Options

This command has no options.

Required Privilege Level

clear

RELATED DOCUMENTATION

show snmp statistics | 2904

List of Sample Output

clear snmp statistics on page 2970

Output Fields

See show snmp statistics for an explanation of output fields.

Sample Output

clear snmp statistics

In the following example, SNMP statistics are displayed before and after the **clear snmp statistics** command is issued:

```
user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 8, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 8, Total set varbinds: 0,
    Get requests: 0, Get nexts: 8, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 2298, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 8, Traps: 2290
```

user@host> **clear snmp statistics**

```

```

user@host> **show snmp statistics**

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

request packet-capture start

Syntax

```
request packet-capture start
<bidirectional bidirectional>
<capture-file capture-file>
<count count>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface>
<maximum-capture-size maximum-capture-size>
<protocol protocol-number>
<size size>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Statement introduced in Junos OS Release 19.3R1.

Description

Captures packet information from the operational mode. You can execute the packet capture from the operational mode with minimal impact to the production system without committing the configurations. You can define the packet filter to trace the type of traffic based on your requirement.

You can request for only one packet capture at a time, and you need to stop each packet capture request before you give an another packet capture request. For each packet capture request, you need to give the respective show command to view the output.

In chassis cluster mode, you must request operational mode packet capture from the primary node. Operational mode packet capture does not function when executed from the secondary node.

Options

bidirectional—Allows to collect bidirectional information.

capture-file—Name of the capture file. It generates a pcap file, which can support Wireshark by adding the suffix '.pcap'.

count—Number of packets to capture.

Range: 10 through 1000000

Default: 100

destination-port—TCP/UDP destination port.

destination-prefix—Destination IPv4/IPv6 address prefix to filter the packets.

interface—Name of the logical interface.

maximum-capture-size—The maximum size of packet capture. The packet truncates if the capture size is more than the specified capture size.

Range: 68 through 10000

Default: 1514

protocol-number—Numeric protocol value.

Range: 0 through 255

Default: 0

size—The maximum size of packet capture file.

Range: 10240 through 1073741824

Default: 50M

source-port—TCP/UDP source port.

source-prefix—Source IPv4/IPv6 address prefix to filter the packets.

Required Privilege Level
view

RELATED DOCUMENTATION

Packet Capture from Operational Mode | **1629**

List of Sample Output

Packet capture using protocol, destination port, destination prefix, and bidirectional options on page 2975
Packet capture using interface on page 2975
Packet capture using source prefix on page 2976
Packet capture using source port on page 2976
Packet capture using protocol on page 2976

Output Fields

Table 274 on page 2973 lists the output fields for the **request packet-capture start** command. Output fields are listed in the approximate order in which they appear.

Table 274: request packet-capture start Output Fields

Field Name	Field Description
packet capture is running	Status of the packet capture session: • **0**: No packet capture is performing. • **1**: Packet capture is performing.

Table 274: request packet-capture start Output Fields *(continued)*

Field Name	Field Description
counter of packet capture	Number of packets captured.
packet capture capture-file name	Name, location, size and capture length of the packet capture file.
Flag	Decimal value corresponding to the type of filter configured. Convert this value to binary or hexadecimal format such as: • 0x000 (No filters) • 0x001 (Source IP) • 0x002 (Destination IP) • 0x004 (Protocol) • 0x008 (Source port) • 0x010 (Destination port) • 0x040 (Filter is valid) • 0x200 (IPv6 Source IP) • 0x400 (IPv6 Destination IP) • 0x800 (Interface) For example if the flag value is **72**, convert it to binary or hexadecimal format: 72 = 0x48 • 0x040 (Filter is valid) • 0x008 (Source port) This means that the filter is valid and only configured with the filter source port.
Source	Source IPv4/IPv6 address.
Destination	Destination IPv4/IPv6 address.
Interface	Name of the logical interface.
bidirectional	Status of the bidirectional keyword configuration: • **0**: Not configured. • **1**: Configured.
Protocol	Numeric protocol value.

Table 274: request packet-capture start Output Fields *(continued)*

Field Name	Field Description
rotate	Number of capture files.
snap_len	The maximum packet capture size.
ifl	If index value of interface.

Sample Output

Packet capture using protocol, destination port, destination prefix, and bidirectional options

`root@host>` **request packet-capture start protocol 17 destination-port 53 destination-prefix 203.0.113.0 bidirectional**

```
{primary:node1}
```

`root@host>` **show packet-capture status**

```
    packet capture is running: 1
    counter of packet capture: 100
    packet capture capture-file name: /var/log/packet-capture.pcap size: 52428800
 rotate: 0 snap_len: 1514
  bidirectional: 1
    Flag: 86 Protocol: udp
    Source: 0.0.0.0 0.0.0.0 (port 0~65535)
    Destination: 203.0.113.0 255.255.255.255 (port 53~53)
    Interface: None ifl: 0
     Flag: 77 Protocol: udp
    Source: 203.0.113.0 255.255.255.255 (port 53~53)
    Destination: 0.0.0.0 0.0.0.0 (port 0~65535)
    Interface: None ifl: 0
```

Packet capture using interface

`user@host>` **request packet-capture start capture-file cli-e2e interface xe-1/0/2.0**

`user@host>` **show packet-capture status**

```
packet capture is running: 1
    counter of packet capture: 100
```

```
   packet capture capture-file name: /var/log/cli-e2e.pcap size: 52428800 rotate:
0 snap_len: 1514
 bidirectional: 0
   Flag: 2112
   Source: 0.0.0.0 0.0.0.0 (port 0~65535)
   Destination: 0.0.0.0 0.0.0.0 (port 0~65535)
   Interface: xe-1/0/2.0 ifl: 68
```

Packet capture using source prefix

`user@host>` **request packet-capture start capture-file cli-e2e source-prefix 192.0.2.0**

`user@host>` **show packet-capture status**

```
packet capture is running: 1
counter of packet capture: 100
packet capture capture-file name: /var/log/cli-e2e.pcap size: 52428800 rotate: 0
snap_len: 1514
bidirectional: 0
Flag: 65
Source: 192.0.2.0.2 255.255.255.255 (port 0~65535)
Destination: 0.0.0.0 0.0.0.0 (port 0~65535)
Interface: None ifl: 0
```

Packet capture using source port

`user@host>` **request packet-capture start capture-file cli-e2e count 100 source-port telnet**

`user@host>` **show packet-capture status**

```
packet capture is running: 1
counter of packet capture: 100
packet capture capture-file name: /var/log/cli-e2e.pcap size: 52428800 rotate: 0
snap_len: 1514
bidirectional: 0
Flag: 72
Source: 0.0.0.0 0.0.0.0 (port 23~23)
Destination: 0.0.0.0 0.0.0.0 (port 0~65535)
Interface: None ifl: 0
```

Packet capture using protocol

`user@host>` **request packet-capture start protocol 6**

user@host> **show packet-capture status**

```
packet capture is running: 1
counter of packet capture: 100 packet
capture capture-file name: /var/log/packet-capture.pcap size: 52428800 rotate: 0
snap_len: 1514
bidirectional: 0
Flag: 68
Protocol: tcp
Source: 0.0.0.0 0.0.0.0 (port 0~65535)
Destination: 0.0.0.0 0.0.0.0 (port 0~65535)
Interface: None ifl: 0
```

request packet-capture stop

Syntax

```
request packet-capture stop
```

Release Information

Statement introduced in Junos OS Release 19.3R1.

Description

Stops the packet capture request from the operational mode. You can execute the packet capture from the operational mode with minimal impact to the production system without committing the configurations. You must stop the packet capture request to generate the packet capture report.

Required Privilege Level

view

RELATED DOCUMENTATION

Packet Capture from Operational Mode | 1629

request packet-capture start | 2972

List of Sample Output

request packet-capture stop on page 2978

Output Fields

This command produces no output.

Sample Output

request packet-capture stop

```
user@host> request packet-capture stop
```

request pppoe connect

Syntax

```
request pppoe connect
```

Release Information

Statement supported on SRX300, SRX320, SRX340, and SRX345 is introduced in Junos OS Release 15.1X49-D60.

Statement supported on SRX1500 and vSRX instances is introduced in Junos OS Release 15.1X49-D100.

Description

Connect all sessions that are down.

Options

pppoe interface name— (Optional) Connect to a specified session.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

> *Understanding PPPoE Interfaces*
>
> *Example: Configuring PPPoE Interfaces*

List of Sample Output

request pppoe connect on page 2979

Output Fields

When you enter this command, this command returns no output.

Sample Output

request pppoe connect

```
user@host> request pppoe connect
```

request pppoe disconnect

Syntax

```
request pppoe disconnect
```

Release Information
Statement supported on SRX300, SRX320, SRX340, and SRX345 is introduced in Junos OS Release 15.1X49-D60.
Statement supported on SRX1500 and vSRX instances is introduced in Junos OS Release 15.1X49-D100.

Description
Disconnect all active sessions.

Options
session id — (Optional) Disconnect the session for which the session ID is specified.

pppoe interface name— (Optional) Disconnect the session for a specific pppoe interface name.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

> *Understanding PPPoE Interfaces*
>
> *Example: Configuring PPPoE Interfaces*

List of Sample Output
request pppoe disconnect on page 2980

Output Fields
When you enter this command, this command returns no output.

Sample Output

request pppoe disconnect

```
user@host> request pppoe disconnect
```

request services ip-monitoring preempt-restore policy

Syntax

```
request services ip-monitoring preempt-restore policy
<policy-name>
```

Release Information

Command introduced in Junos OS Release 11.4.

Description

If the no–preempt option is specified, the policy will not perform preemptive failback when it is in a failover state, and when the RPM probe test recovers from failure. To manually revert to the failback state, run the **request services ip-monitoring preempt-restore policy** command.

> **NOTE:** The **request services ip-monitoring preempt-restore policy** command takes effect only when the RPM probe is in the pass state, and when the policy is in a failover state.

Options

policy name—Name of the policy.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

show services ip-monitoring status | 3051

List of Sample Output

run request services ip-monitoring preempt-restore policy <policy name> on page 2981

Output Fields

When you run this command, the policy is restored to the failback state.

Sample Output

run request services ip-monitoring preempt-restore policy <policy name>

```
user@host> run request services ip-monitoring preempt-restore policy policy1
```

```
Restore request succeeded: Policy policy1
```

request services rpm twamp start

Syntax

```
request services rpm twamp start client <control-connection-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Start the probes of a Two-Way Active Measurement Protocol (TWAMP) client. You can start all sessions for all TWAMP clients, or start a session for a specific TWAMP client. When you start test session configured for a particular TWAMP client, the control client initiates all requested testing with a start-sessions message, and the server sends an acknowledgment. If the control connection is not active between the server and the client, the control connection is also established and the test connections are started later. If the control client name is not specified, all the configured test sessions are commenced.

Options

start client—Start the TWAMP session between the TWAMP client and the TWAMP server.

control-connection-name—(Optional) Start or stop the TWAMP session with the server only for the specified control connection or TWAMP control client.

Required Privilege Level

view

List of Sample Output

request services rpm twamp start client on page 2983

Output Fields

When you enter this command, you are not provided feedback on the status of your request.

Sample Output

request services rpm twamp start client

```
user@host> request services rpm twamp start client c1
```

request services rpm twamp stop

Syntax

```
request services rpm twamp stop client <control-connection-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Stop the Two-Way Active Measurement Protocol (TWAMP) session between the TWAMP client and the TWAMP server. You can stop all sessions for all TWAMP clients, or stop a session for a specific TWAMP client. When you stop the test session, the control connection is closed only after the stop-sessions message is sent from the TWAMP client to the TWAMP server. If the control client name is not specified, all the configured test sessions are closed.

Options

stop client—Stop the TWAMP session between the TWAMP client and the TWAMP server.

control-connection-name—(Optional) Start or stop the TWAMP session with the server only for the specified control connection or TWAMP control client.

Required Privilege Level

view

List of Sample Output

request services rpm twamp stop client on page 2984

Output Fields

When you enter this command, you are not provided feedback on the status of your request.

Sample Output

request services rpm twamp stop client

```
user@host> request services rpm twamp stop client c1
```

request snmp spoof-trap

Syntax

```
request snmp spoof-trap
<trap> variable-bindings <object> <instance> <value>
```

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 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.

Options

<trap>—Name of the trap to spoof.

variable-bindings <*object*> <*instance*> <*value*>—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, **ifIndex[14] = 14**). Enclose the list of variable bindings in quotation marks (“ “) and use a comma to separate each object name, instance, and value definition (for example, **variable-bindings “ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2”**). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.

<dummy name>—A dummy trap name to display the list of available traps.

Question mark (?)—Question mark**?** to display possible completions.

Required Privilege Level

request

List of Sample Output

request snmp spoof-trap (with Variable Bindings) on page 2986
request snmp spoof-trap (Illegal Trap Name) on page 2986
request snmp spoof-trap (Question Mark ?) on page 2991

Sample Output

request snmp spoof-trap (with Variable Bindings)

user@host> **request snmp spoof-trap linkUp variable-bindings “ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2”**

```
Spoof trap request result: trap sent successfully
```

request snmp spoof-trap (Illegal Trap Name)

user@host> **request snmp spoof-trap xx**

```
Spoof trap request result: trap not found

Allowed Traps:
adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
  adslAtucPerfLolsThreshTrap
  adslAtucPerfLossThreshTrap
  adslAtucPerfLprsThreshTrap
  adslAtucRateChangeTrap
  adslAturPerfESsThreshTrap
  adslAturPerfLofsThreshTrap
  adslAturPerfLossThreshTrap
  adslAturPerfLprsThreshTrap
  adslAturRateChangeTrap
  apsEventChannelMismatch
  apsEventFEPLF
  apsEventModeMismatch
  apsEventPSBF
  apsEventSwitchover
  authenticationFailure
  bfdSessDown
  bfdSessUp
  bgpBackwardTransition
  bgpEstablished
  coldStart
  dlswTrapCircuitDown
  dlswTrapCircuitUp
  dlswTrapTConnDown
  dlswTrapTConnPartnerReject
  dlswTrapTConnProtViolation
```

```
dlswTrapTConnUp
dsx1LineStatusChange
dsx3LineStatusChange
entConfigChange
fallingAlarm
frDLCIStatusChange
ggsnTrapChanged
ggsnTrapCleared
ggsnTrapNew
gmplsTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisIDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAccessAuthServerDisabled
jnxAccessAuthServerEnabled
jnxAccessAuthServiceDown
jnxAccessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared
jnxCollFtpSwitchover
jnxCollMemoryAvailable
jnxCollMemoryUnavailable
jnxCollUnavailableDest
```

```
jnxCollUnavailableDestCleared
jnxCollUnsuccessfulTransfer
jnxDfcHardMemThresholdExceeded
jnxDfcHardMemUnderThreshold
jnxDfcHardPpsThresholdExceeded
jnxDfcHardPpsUnderThreshold
jnxDfcSoftMemThresholdExceeded
jnxDfcSoftMemUnderThreshold
jnxDfcSoftPpsThresholdExceeded
jnxDfcSoftPpsUnderThreshold
jnxEventTrap
jnxExampleStartup
jnxFEBSwitchover
jnxFanFailure
jnxFanOK
jnxFruCheck
jnxFruFailed
jnxFruInsertion
jnxFruOK
jnxFruOffline
jnxFruOnline
jnxFruPowerOff
jnxFruPowerOn
jnxFruRemoval
jnxHardDiskFailed
jnxHardDiskMissing
jnxJsAvPatternUpdateTrap
jnxJsChassisClusterSwitchover
jnxJsFwAuthCapacityExceeded
jnxJsFwAuthFailure
jnxJsFwAuthServiceDown
jnxJsFwAuthServiceUp
jnxJsNatAddrPoolThresholdStatus
jnxJsScreenAttack
jnxJsScreenCfgChange
jnxLdpLspDown
jnxLdpLspUp
jnxLdpSesDown
jnxLdpSesUp
jnxMIMstCistPortLoopProtectStateChangeTrap
jnxMIMstCistPortRootProtectStateChangeTrap
jnxMIMstErrTrap
jnxMIMstGenTrap
jnxMIMstInvalidBpduRxdTrap
```

```
jnxMIMstMstiPortLoopProtectStateChangeTrap
jnxMIMstMstiPortRootProtectStateChangeTrap
jnxMIMstNewRootTrap
jnxMIMstProtocolMigrationTrap
jnxMIMstRegionConfigChangeTrap
jnxMIMstTopologyChgTrap
jnxMacChangedNotification
jnxMplsLdpInitSesThresholdExceeded
jnxMplsLdpPathVectorLimitMismatch
jnxMplsLdpSessionDown
jnxMplsLdpSessionUp
jnxOspfv3IfConfigError
jnxOspfv3IfRxBadPacket
jnxOspfv3IfStateChange
jnxOspfv3LsdbApproachingOverflow
jnxOspfv3LsdbOverflow
jnxOspfv3NbrRestartHelperStatusChange
jnxOspfv3NbrStateChange
jnxOspfv3NssaTranslatorStatusChange
jnxOspfv3RestartStatusChange
jnxOspfv3VirtIfConfigError
jnxOspfv3VirtIfRxBadPacket
jnxOspfv3VirtIfStateChange
jnxOspfv3VirtNbrRestartHelperStatusChange
jnxOspfv3VirtNbrStateChange
jnxOtnAlarmCleared
jnxOtnAlarmSet
jnxOverTemperature
jnxPMonOverloadCleared
jnxPMonOverloadSet
jnxPingEgressJitterThresholdExceeded
jnxPingEgressStdDevThresholdExceeded
jnxPingEgressThresholdExceeded
jnxPingIngressJitterThresholdExceeded
jnxPingIngressStddevThresholdExceeded
jnxPingIngressThresholdExceeded
jnxPingRttJitterThresholdExceeded
jnxPingRttStdDevThresholdExceeded
jnxPingRttThresholdExceeded
jnxPortBpduErrorStatusChangeTrap
jnxPortLoopProtectStateChangeTrap
jnxPortRootProtectStateChangeTrap
jnxPowerSupplyFailure
jnxPowerSupplyOK
```

```
jnxRedundancySwitchover
jnxRmonAlarmGetFailure
jnxRmonGetOk
jnxSecAccessIfMacLimitExceeded
jnxSecAccessdsRateLimitCrossed
jnxSonetAlarmCleared
jnxSonetAlarmSet
jnxSpSvcSetCpuExceeded
jnxSpSvcSetCpuOk
jnxSpSvcSetZoneEntered
jnxSpSvcSetZoneExited
jnxStormEventNotification
jnxSyslogTrap
jnxTemperatureOK
jnxVccpPortDown
jnxVccpPortUp
jnxVpnIfDown
jnxVpnIfUp
jnxVpnPwDown
jnxVpnPwUp
jnxl2aldGlobalMacLimit
jnxl2aldInterfaceMacLimit
jnxl2aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange
mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp
mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecIllglLblThrshExcd
mplsTunnelDown
mplsTunnelReoptimized
mplsTunnelRerouted
mplsTunnelUp
```

```
mplsVrfIfDown
mplsVrfIfUp
mplsXCDown
mplsXCUp
msdpBackwardTransition
msdpEstablished
newRoot
ospfIfAuthFailure
ospfIfConfigError
ospfIfRxBadPacket
ospfIfStateChange
ospfLsdbApproachingOverflow
ospfLsdbOverflow
ospfMaxAgeLsa
ospfNbrStateChange
ospfOriginateLsa
ospfTxRetransmit
ospfVirtIfAuthFailure
ospfVirtIfConfigError
ospfVirtIfRxBadPacket
ospfVirtIfStateChange
ospfVirtIfTxRetransmit
ospfVirtNbrStateChange
pethMainPowerUsageOffNotification
pethMainPowerUsageOnNotification
pethPsePortOnOffNotification
pingProbeFailed
pingTestCompleted
pingTestFailed
ptopoConfigChange
risingAlarm
rpMauJabberTrap
sdlcLSStatusChange
sdlcPortStatusChange
topologyChange
traceRoutePathChange
traceRouteTestCompleted
traceRouteTestFailed
vrrpTrapAuthFailure
vrrpTrapNewMaster
warmStart
```

request snmp spoof-trap (Question Mark ?)

`user@host>` **request snmp spoof-trap ?**

```
Possible completions:
  <trap>               The name of the trap to spoof
  adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
  adslAtucPerfLolsThreshTrap
  adslAtucPerfLossThreshTrap
  adslAtucPerfLprsThreshTrap
  adslAtucRateChangeTrap
  adslAturPerfESsThreshTrap
  adslAturPerfLofsThreshTrap
  adslAturPerfLossThreshTrap
  adslAturPerfLprsThreshTrap
  adslAturRateChangeTrap
  apsEventChannelMismatch
  apsEventFEPLF
  apsEventModeMismatch
  apsEventPSBF
  apsEventSwitchover
  authenticationFailure
  bfdSessDown
  bfdSessUp
  bgpBackwardTransition
  bgpEstablished
  coldStart
  dlswTrapCircuitDown
  dlswTrapCircuitUp
---(more 10%)---
```

request snmp utility-mib set instance

Syntax

```
request snmp utility-mib set instance name
object-type type
object-value value
```

Release Information

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

Store data in the specified container object in the SNMP Utility MIB. The data may be retrieved by SNMP operations.

Options

name—Name of the SNMP instance that is used to identify the data stored in the container object.

object-type *type*—Type of container object in which to store data. The following container object types are supported:

- **counter**—Stores a 32-bit counter value.
- **counter64**—Stores a 64-bit counter value.
- **integer**—Stores a 32-bit signed integer value.
- **unsigned-integer**—Stores a 32-bit unsigned integer value.
- **string**—Stores an octet string value.

object-value *value*—Data that is stored in the container object.

Required Privilege Level

request

RELATED DOCUMENTATION

Utility MIB | 615

Understanding the Implementation of SNMP on the QFabric System

request snmp utility-mib clear instance | 2994

request snmp utility-mib clear instance

Syntax

```
request snmp utility-mib clear instance name
object-type type
```

Release Information

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 the data stored in the specified container object in the SNMP Utility MIB.

Options

name—Name of the SNMP instance that is used to identify the data stored in the container object.

object-type *type*—Type of container object in which the data is stored. The following container object types are supported:

- **counter**—Stores a 32-bit counter value.
- **counter64**—Stores a 64-bit counter value.
- **integer**—Stores a 32-bit signed integer value.
- **unsigned-integer**—Stores a 32-bit unsigned integer value.
- **string**—Stores an octet string value.

Required Privilege Level

clear

RELATED DOCUMENTATION

Utility MIB | 615

Understanding the Implementation of SNMP on the QFabric System

request snmp utility-mib set instance | 2993

request support information

List of Syntax

Syntax on page 2995
Syntax (SRX Series devices) on page 2995
Syntax (EX Series Switch) on page 2995
Syntax (MX Series Router) on page 2995
Syntax (TX Matrix Router) on page 2995
Syntax (TX Matrix Plus Router) on page 2996

Syntax

```
request support information
<brief>
```

Syntax (SRX Series devices)

```
request support information
<brief>
<secure-gateway>
<security-components>
```

Syntax (EX Series Switch)

```
request support information
<brief>
<all-members>
<local>
<member member-id>
```

Syntax (MX Series Router)

```
request support information
<brief>
<all-members>
<local>
<member member-id>
<ipsec-vpn>
```

Syntax (TX Matrix Router)

```
request support information
<brief>
<all-lcc | lcc number | scc>
```

Syntax (TX Matrix Plus Router)

```
request support information
<brief>
<all-chassis | all-lcc | lcc number | sfc number>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **brief** introduced in Junos OS Release 13.2.
Option **secure-gateway** introduced in Junos OS Release 15.1X49-D110 for SRX5400, SRX5600, and SRX5800 devices.
Options **security-components** and **ipsec-vpn** introduced in Junos OS Release 20.2R1.

Description

Display all configuration data for the system, including data hidden with the **apply-flags omit** command. Issue this command before contacting customer support, and then include the command output in your support request. Output from this command varies somewhat, depending on which platform you issue the command from. However, the command always executes a series of **show** commands, with the appropriate information for your device automatically included.

Options

brief—(Optional) Display brief information for the command output. Without this option, display of the output can take a long time to complete.

all-chassis—(TX Matrix and TX Matrix Plus routers) (Optional) Display system information for all chassis.

all-lcc—(TX Matrix and TX Matrix Plus routers) (Optional) On a TX Matrix router, display system information for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display system information for all chassis for all T1600 or T4000 routers (or line-card chassis) connected to the TX Matrix Plus router.

all-members—(EX Series switches and MX Series routers) (Optional) Display system information for all members of the Virtual Chassis configuration.

lcc *number*—(TX Matrix and TX Matrix Plus routers) (Optional) On a TX Matrix router, display system information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system storage information for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX Series switches and MX Series routers) (Optional) Display system information for the local Virtual Chassis member.

member *member-id*—(EX Series switches and MX Series routers) (Optional) Display system information for the specified member of the Virtual Chassis configuration. On EX Series switches, replace ***member-id*** with a value appropriate for that Virtual Chassis configuration. On MX Series routers, replace ***member-id*** with a value of 0 or 1.

scc—(TX Matrix routers) (Optional) Display system information for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers) (Optional) Display system information for the TX Matrix Plus router (or switch-fabric chassis). Replace ***number*** with **0**.

secure-gateway—(SRX5400, SRX5600, and SRX5800 devices) (Optional) Display system information for secure gateway deployment scenarios.

security-component—(SRX Series) (Optional) Display information on security components.

- **ipsec-vpn**—Generate security report for IPsec VPN.

node—(SRX5400, SRX5600, and SRX5800 devices) (Optional) Display detailed system status report for all nodes or a specific node.

- ***node-id***—Display detailed system status report for a specific node. Replace ***node-id*** with a value of 0 or 1.
- **all**—Display detailed system status report for all nodes.
- **local**—Display detailed system status report for the local node.
- **primary**—Display detailed system status report for the primary node.

Additional Information

The **show** commands issued as a result of this command vary depending on which platform you issue the command from. Output is always appropriate for the device. For example, Table 275 on page 2998 lists the **show** commands that are called when you issue **request support information** on an MX Series router.

Table 275: Sample show Commands Called by the request support information command on an MX Series Router

show chassis alarms no-forwarding	show interfaces extensive no-forwarding
show chassis environment no-forwarding	show krt queue
show chassis fabric degradation	show krt state
show chassis fabric destinations	show pfe statistics error
show chassis fabric fpcs	show pfe statistics traffic
show chassis fabric plane	show route summary
show chassis fabric reachability	show system boot-messages no-forwarding
show chassis fabric summary	show system buffer no-forwarding
show chassis fpc	show system commit
show chassis fpc detail	show system core-dumps no-forwarding
show chassis firmware no-forwarding	show system processes extensive no-forwarding
show chassis hardware detail no-forwarding	show system queues no-forwarding
show chassis hardware extensive no-forwarding	show system statistics no-forwarding
show pfe statistics traffic	show system storage no-forwarding
show chassis power	show system uptime no-forwarding
show chassis routing-engine no-forwarding	show system virtual-memory no-forwarding
show configuration | except SECRET-DATA	show version detail no-forwarding

NOTE: Show command **show interfaces extensive no-formwarding** is not supported for **request support information brief** command.

The **no-forwarding** option ensures that all mgd processes associated with the **show** command are properly halted if you break into the output (Ctrl+C) while the command is still running.

> **NOTE:** The **no-forwarding** option ensures that all mgd processes associated with the **show** command are properly halted if you break into the output (Ctrl+C) while the command is still running.

Table 276 on page 2999 lists the **show** commands that are called when you issue **request support information ipsec-vpn** on a MX Series Router.

Table 276: Sample show commands called by the request support information ipsec-vpn command on an MX Series Router

show version no-forwarding | no-more	show services ipsec-vpn ipsec statistics | no-more
show system uptime no-forwarding | no-more	show security pki local-certificate detail no-forwarding
show system core-dumps no-forwarding | no-more	show security pki local-certificate system-generated detail no-forwarding
show system processes extensive no-forwarding | grep ike	show security pki ca-certificate detail no-forwarding
show system processes extensive no-forwarding | grep kmd	show security pki crl detail no-forwarding
show chassis fpc pic-status	show security pki certificate-request detail no-forwarding
show chassis cluster status	show security pki statistics no-forwarding | no-more
show chassis cluster interfaces	show ipsec memory-usage | no-more
show chassis cluster information	show services sessions analysis | no-more
show configuration | no-more	show services sessions extensive | no-more
show route forwarding-table | no-more	show pfe statistics traffic | no-more
show interfaces extensive | no-more	show pfe statistics exceptions | no-more
show services ipsec-vpn ike security-associations detail | no-more	show pfe statistics error | no-more
show services ipsec-vpn ike statistics | no-more	show extension-provider system processes extensive | match mspmand

Table 276: Sample show commands called by the request support information ipsec-vpn command on an MX Series Router *(continued)*

show services ipsec-vpn ipsec security-associations detail | no-more	**show services service-sets statistics packet-drops | no-more**
plugin ipsec show stats all	**plugin ipsec show sadb detail**
plugin ipsec show rules all	**plugin ipsec show rules no-sa**
plugin ipsec show sa-trigger-seqno	**plugin ipsec show invalid-spi brief**
plugin ipsec show invalid-spi history	**show msp pkt-cntrs terse**
show msp pkt-cntrs	**show msp plugins pkt-cntrs**
show msp service-sets	**show msp service-sets summary**
show msp service-sets mem-usage	**show msp ip-stats**
show msp mem usage	**show msp mem ocwm jnx-msp-shm-data mum**
show msp mem ocwm jnx-msp-shm-data mum objcache	**show msp stats ctrl**
show msp cpu-throttle	**show svcs-xlp intf counters**
show svcs-xlp exceptions	**show svcs-xlp exceptions detail**
show svcs-xlp cpu stats	**show svcs-xlp fifo**
show svcs-xlp poe stats	**show svcs-xlp jbuf-stats**
plugin ha show ckpt	**plugin ha show ha-pvt-obj stats**
plugin ha show info-ha-plugin	**plugin ha show stats**
plugin ha show udp	**plugin ha show mtu**
plugin ha show junos-sync stats	**plugin ha show junos-sync stats aggregation**
plugin ha show junos-sync stats history	

Starting in Release 20.2R1, Junos OS introduces **ipsec-vpn** option to the existing **request support information** command. The **request support information ipsec-vpn** command displays all the configurations,

states, and statistics at Routing Engine and Service Card level. This new option helps in debugging IPsec-VPN related issues. The information collection is streamlined and reduces the output file size.

Table 277 on page 3001 lists the **show** commands that are called when you issue **request support information** on an EX Series 9200 switch. The table does not include the **no-forwarding** option, which is used for purposes of the **request support information**, itself.

Table 277: Sample show Commands Called by the request support information command on an EX Series 9200 Switch

show chassis alarms	**show interfaces extensive**
show chassis environment	
show chassis firmware	**show pfe statistics traffic**
*show chassis fpc*detail	**show spanning-tree bridge detail**
show chassis hardware detail	**show spanning-tree interface**
show chassis routing-engine	
show configuration | except SECRET-DATA | display omit	**show system boot-messages**
show dhcp-security binding	**show system queues**
show dhcp-security ipv6 binding	**show system processes extensive**
	show system queues
show ethernet-switching interface detail	**show system statistics**
show ethernet-switching table	**show vlans extensive**
	show vrrp summary

Table 278 on page 3001 lists the **show** commands that are called when you issue **request support information** on SRX Series devices.

Table 278: Sample show Commands Called by the request support information command on SRX Series devices

show pfe statistics traffic	**show interfaces queue**
show chassis environment no-forwarding	**show security monitoring fpc 0**

Table 278: Sample show Commands Called by the request support information command on SRX Series devices *(continued)*

show chassis fpc detail	show system license
show system storage no-forwarding	show security policies hit-count no-forwarding
show system virtual-memory no-forwarding	show security policies information no-forwarding
show system buffer no-forwarding	show security dns-cache
show system queues no-forwarding	show security flow statistics
show chassis hardware extensive no-forwarding	show security flow status
show krt queue	show security flow session summary no-forwarding
show route summary	show security utm anti-virus status
show version no-forwarding	show system processes extensive no-forwarding
show system uptime no-forwarding	show chassis fpc pic-status
show system core-dumps no-forwarding	show chassis cluster status
show chassis cluster interfaces	show chassis cluster information
show route forwarding-table	show interfaces extensive
show security pki local-certificate detail no-forwarding	show security pki local-certificate system-generated detail no-forwarding
show security pki ca-certificate detail no-forwarding	show security pki crl detail no-forwarding
show security pki certificate-request detail no-forwarding	show security pki statistics no-forwarding
show security internal-security-association no-forwarding	show security ike security-associations detail no-forwarding
show security ike active-peer stats no-forwarding	show security ike stats no-forwarding
show security ipsec security-associations detail no-forwarding	show security ipsec statistics no-forwarding

Table 278: Sample show Commands Called by the request support information command on SRX Series devices *(continued)*

show security ipsec tunnel-distribution no-forwarding	**show security ipsec tunnel-distribution summary no-forwarding**
show security ipsec next-hop-tunnels no-forwarding	**show security ipsec tunnel-events-statistics no-forwarding**
show security ipsec inactive-tunnels no-forwarding	**show pfe statistics traffic**
show usp ipsec sa	**show usp ipsec pmi-sa**
show usp ipsec global-stat	**show usp ipsec pkt-stat**
show usp ipsec stat	**show usp ipsec spd table**
show usp ipsec spd stats	**show usp ipsec traffic-selector stats**
show usp ipsec traffic-selector pkt-stats	**show usp ipsec tunnel-distribution**
show usp ipsec nsp-tunnel-table	**show usp ipsec nhtb**
show usp ipsec ager stats	**show talus *number* stats all**
show talus *number* drop-pkt	**show talus *number* queue-bp**
show jspec talus *number* registers cntr fi_bp *number*	**show jspec talus *number* registers cntr fi_bp *number***
show jspec talus *number* registers cntr fi_bp *number*	**show jspec talus *number* registers cntr fi_bp *number***
show jspec talus *number* registers cntr fo_free *number*	**show jspec talus *number* registers cntr fo_free *number***
show jspec talus *number* registers cntr fo_free *number*	**show jspec talus *number* registers cntr fo_free *number***
show jspec talus *number* registers cntr ing_eop *number*	**show jspec talus *number* registers cntr ing_eop *number***
show jspec talus *number* registers cntr ing_eop *number*	**show jspec talus *number* registers cntr ing_eop *number***

Starting in Junos OS Release 15.1X49-D110, on SRX5400, SRX5600, and SRX5800 devices, a new option **secure-gateway** is added to the existing **request support information** command. This new option displays all the required information that is relevant for secure gateway deployment scenarios. In Junos OS Release 15.1X49-D100 and earlier, request support information displays the information about all features that might not be relevant for secure gateway deployments.

Starting in Junos OS Release 20.2R1, we've introduced the CLI **ipsec-vpn** option to the existing **request support information security-components** command. This new option displays all the configuration, states, and statistics information necessary for debugging IPsec VPN related issues.

Required Privilege Level
maintenance

List of Sample Output
request support information | save on page 3004
request support information scc (TX Matrix Router) on page 3004
request support information sfc (TX Matrix Plus Router) on page 3006
request support information (SRX Series device) on page 3009
request support information ipsec-vpn (MX Series Router) on page 3010

Output Fields
For information about output fields, see the description for the specific command--listed in the output–in which you are interested.

Sample Output

request support information | save

```
user@host> request support information | save hostA
```

```
Wrote 1143 lines of output to 'hostA'
```

```
user@host>
```

request support information scc (TX Matrix Router)

```
user@host> request support information scc
```

```

```

```
user@host> show system uptime
```

```

scc-re0:
--------------------------------------------------------------------------
Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 12:53:26 PDT (11:55:40 ago)
```

```
Protocols started: 2004-09-14 12:54:19 PDT (11:54:47 ago)
Last configured: 2004-09-14 13:07:47 PDT (11:41:19 ago) by user
12:49AM PDT up 11:56, 3 users, load averages: 0.00, 0.02, 0.03

lcc0-re0:
--------------------------------------------------------------------------
Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 15:36:41 PDT (09:12:25 ago)
Last configured: 2004-09-14 15:38:06 PDT (09:11:00 ago) by root
12:49AM PDT up 9:12, 0 users, load averages: 0.13, 0.05, 0.02

lcc2-re0:
--------------------------------------------------------------------------
Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 15:36:47 PDT (09:12:19 ago)
Last configured: 2004-09-14 15:38:09 PDT (09:10:57 ago) by root
12:49AM PDT up 9:12, 0 users, load averages: 0.00, 0.00, 0.00
```

user@host> **show version**

```
scc-re0:
--------------------------------------------------------------------------
Hostname: hostA
Model: TX Matrix
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]
JUNOS Support Tools Package [7.0-20040908.0]

lcc0-re0:
--------------------------------------------------------------------------
Hostname: hostB
Model: t640
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
```

```
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]

lcc2-re0:
--------------------------------------------------------------------------
Hostname: dewey
Model: t640
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]
...
```

request support information sfc (TX Matrix Plus Router)

user@host> **request support information sfc 0**

```
sfc0-re0:
--------------------------------------------------------------------------

root@host> show system uptime no-forwarding

Current time: 2009-05-25 03:43:28 PDT
System booted: 2009-05-25 01:15:04 PDT (02:28:24 ago)
Protocols started: 2009-05-25 01:16:01 PDT (02:27:27 ago)
Last configured: 2009-05-25 03:03:42 PDT (00:39:46 ago) by user
 3:43AM  up 2:28, 7 users, load averages: 0.00, 0.00, 0.00


root@host> show version detail no-forwarding

Hostname: aj
Model: txp
JUNOS Base OS boot [9.6-20090519.0]
JUNOS Base OS Software Suite [9.6-20090519.0]
JUNOS Kernel Software Suite [9.6-20090519.0]
...
root@host> show system core-dumps no-forwarding

-rw-------  1 root  wheel  152223744 May 25 03:10 /var/crash/vmcore.0
-rw-r--r--  1 bdeleon field    139417 May 22 10:17
```

```
/var/tmp/aj-core-apps-config-n-gres.txt
...
root@host> show chassis alarms no-forwarding

9 alarms currently active
Alarm time               Class  Description
2009-05-25 01:27:08 PDT  Minor  LCC 0 Minor Errors
2009-05-25 01:27:08 PDT  Minor  Spare SIB F13 6 Fault
...
root@host> show chassis hardware detail no-forwarding

Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN112F007AHB      TXP
Midplane         REV 05   710-022574   TS4027            SFC Midplane
FPM Display      REV 03   710-024027   DX0282            TXP FPM Display
...
root@host> show system processes extensive no-forwarding

last pid:  6639;  load averages:  0.00,  0.00,  0.00  up 0+02:28:54    03:43:28
161 processes: 5 running, 138 sleeping, 18 waiting

Mem: 236M Active, 227M Inact, 104M Wired, 392M Cache, 69M Buf, 2296M Free
Swap: 2048M Total, 2048M Free


  PID USERNAME     THR PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
   11 root           1 171   52     0K    12K RUN    143:00 96.78% idle
 1530 root           1  96    0 38160K 24812K select   2:54  1.12% chassisd
 1343 root           1  76    0     0K    12K          0:18  0.00% bcmLINK.0
 1345 root           1  76    0     0K    12K          0:15  0.00% brq17: uhci1
uhci*
...
root@host> show pfe statistics error


Slot 4

SLCHIP Error statistics:

SLCHIP                 0        1
-------------------------------------------------------
Lin XIF      :         0        0
Lin SRCTL    :         0        0
```

```
...
root@host>show pfe statistics traffic

Packet Forwarding Engine traffic statistics:
    Input  packets:              2590754                    0 pps
    Output packets:              2640010                    0 pps
Packet Forwarding Engine local traffic statistics:
    Local packets input                :              2064527
    Local packets output               :              2115925
    Software input control plane drops  :                    0
    Software input high drops          :                    0
    Software input medium drops        :                    0
    Software input low drops           :                    0
    Software output drops              :                    0
    Hardware input drops               :                    0
Packet Forwarding Engine local protocol statistics:
    HDLC keepalives            :                     0
    ATM OAM                    :                     0
    Frame Relay LMI            :                     0
    PPP LCP/NCP                :                     0
    OSPF hello                 :                 20048
    OSPF3 hello                :                   109
    RSVP hello                 :                  3485
    LDP hello                  :                  7191
    BFD                        :                     0
    IS-IS IIH                  :                 11318
    LACP                       :                     0
    ARP                        :                   629
    ETHER OAM                  :                   930
    Unknown                    :                 13212
Packet Forwarding Engine hardware discard statistics:
    Timeout                    :                     0
    Truncated key              :                     0
    Bits to test               :                     0
    Data error                 :                     0
    Stack underflow            :                     0
    Stack overflow             :                     0
    Normal discard             :                 18060
    Extended discard           :                     0
    Invalid interface          :                     0
    Info cell drops            :                     0
    Fabric drops               :                     0
Packet Forwarding Engine Input IPv4 Header Checksum Error and Output MTU Error
statistics:
```

```
    Input Checksum             :                    0
    Output MTU                 :                    0

root@host> show chassis routing-engine no-forwarding

Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 32 degrees C / 89 degrees F
    CPU temperature             46 degrees C / 114 degrees F
    DRAM                      3327 MB
...
root@host> show chassis environment no-forwarding

Class Item                           Status     Measurement
Temp  PEM 0                          OK         30 degrees C / 86 degrees F
...
root@host> show chassis firmware no-forwarding

Part                     Type       Version
Global FPC 4
Global FPC 6
Global FPC 7
...
root@host> show system boot-messages  no-forwarding
...
```

request support information (SRX Series device)

`user@host>` **request support information**

```
root@host> show security dns-cache
DNS entry number: 0

root@host> show security utm web-filtering statistics

 UTM web-filtering statistics:
    Web-filtering sessions in total:    512000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                       0              0
          Timeout                       0              0
     Connectivity                       0              0
```

```
Too-many-requests                       0              0

root@host> show security utm session

 UTM session info:
 Maximum sessions:               256000
 Total allocated sessions:       0
 Total freed sessions:           0
 Active sessions:                0

root@host> show system uptime no-forwarding

Current time: 2017-07-09 21:38:01 PDT
Time Source:  LOCAL CLOCK
System booted: 2017-07-09 20:58:06 PDT (00:39:55 ago)
Protocols started: 2017-07-09 20:58:07 PDT (00:39:54 ago)
Last configured: 2017-06-30 08:56:45 PDT (1w2d 12:41 ago) by user
 9:38PM  up 40 mins, 1 user, load averages: 0.10, 0.07, 0.04
...
```

request support information ipsec-vpn (MX Series Router)

`user@host>` **request support information ipsec-vpn**

```
root@mobst480e> show services ipsec-vpn ike security-associations detail | no-more
IKE peer 10.0.1.2
  Role: Responder, State: Matured
  Initiator cookie: 9425c926b3614be5, Responder cookie: 1bcf54a314423b3f
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local gateway interface: ge-4/3/3.0
  Local: 10.0.1.1, Remote: 10.0.1.2
  Lifetime: Expires in 1923 seconds
  Peer ike-id: ipv4(any:0,[0..3]=10.0.1.2)
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
   Diffie-Hellman group  : 2
  Traffic statistics:
   Input  bytes  :                 8024
   Output bytes  :                 7744
   Input  packets:                   52
   Output packets:                   52
  Flags: IKE SA created
```

```
  IPSec security associations: 34 created, 36 deleted

root@mobst480e> show services ipsec-vpn ike statistics | no-more
IKE peer 10.0.1.2
  Initiator cookie: 9425c926b3614be5, Responder cookie: 1bcf54a314423b3f
  Local: 10.0.1.1, Remote: 10.0.1.2
  IPSec security associations: 34 created, 36 deleted
  IPSec tunnel rekeys: 17
  Exchange type: IKEv2
  Traffic statistics:
   Input  bytes  :                                  8024
   Output bytes  :                                  7744
   Input  packets:                                    52
   Output packets:                                    52
  Delete IPsec SA payload statistics:
   Delete IPsec SA payloads received:                 18
   Delete IPsec SA payloads sent    :                 17
  DPD statistics:
   DPD request received          :                    18
   DPD request sent              :                     0
   DPD response received         :                     0
   DPD response sent             :                    18
   DPD response missed           :                     0
   Worst case DPD response delay  :                    0 msec
   DPD sequential response missed :                    0
  Invalid SPI notification statistics:
   Notifications received:                            0
   Notifications sent    :                            0

root@mobst480e> show services ipsec-vpn ipsec security-associations detail | no-more
Service set: ss1, IKE Routing-instance: default

  Rule: ipsec_vpn_rules_1, Term: term1, Tunnel index: 1
  Local gateway: 10.0.1.1, Remote gateway: 10.0.1.2
  IPSec inside interface: ms-2/0/0.1, Tunnel MTU: 1500
  UDP encapsulate: Disabled, UDP Destination port: 0
  Local identity: ipv4_subnet(any:0,[0..7]=192.168.60.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=192.168.70.0/24)
  NATT Detection: Not Detected, NATT keepalive interval: 0
  Total uptime:  0 days 2 hrs 45 mins 21 secs

    Direction: inbound, SPI: 2957881284, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
```

```
    Soft lifetime: Expires in 48 seconds
    Hard lifetime: Expires in 88 seconds
    Anti-replay service: Enabled, Replay window size: 4096
    Copy ToS: Enabled
    Copy TTL: Disabled, TTL value: 64
    SA lifetime: 180 seconds

    Direction: outbound, SPI: 3292864325, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 48 seconds
    Hard lifetime: Expires in 88 seconds
    Anti-replay service: Enabled, Replay window size: 4096
    Copy ToS: Enabled
    Copy TTL: Disabled, TTL value: 64
    SA lifetime: 180 seconds

root@mobst480e> show services ipsec-vpn ipsec statistics | no-more

PIC: ms-2/0/0, Service set: ss1

ESP Statistics:
  Encrypted bytes:               0
  Decrypted bytes:               0
  Encrypted packets:             0
  Decrypted packets:             0
AH Statistics:
  Input bytes:                   0
  Output bytes:                  0
  Input packets:                 0
  Output packets:                0
Errors:
  AH authentication failures:    0
  ESP authentication failures:   0
  ESP decryption failures:       0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

show chassis alarms

Syntax

```
show chassis alarms
```

Release Information
Command introduced in Junos OS Release 11.1 for SRX Series devices.

Description
Display information about the conditions that have been configured to trigger alarms.

Options
This command has no options.

Additional Information
Chassis alarms are preset. You cannot modify them.

You cannot clear the alarms for chassis components. Instead, you must remedy the cause of the alarm. When a chassis alarm is lit, it indicates that you are running the device in a manner that we do not recommend.

On routers, you can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button, located on the craft interface. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after you silence an external device reactivate the external device.

In Junos OS Release 11.1 and later, alarms for fans also show the slot number of the fans in the CLI output.

Required Privilege Level
view

RELATED DOCUMENTATION

show system alarms | 3118

List of Sample Output
show chassis alarms on page 3014

Output Fields
Table 279 on page 3014 lists the output fields for the **show chassis alarms** command. Output fields are listed in the approximate order in which they appear.

Table 279: show chassis alarms Output Fields

Field Name	Field Description
Alarm time	Date and time the alarm was first recorded.
Class	Severity class for this alarm: Minor or Major.
Description	Information about the alarm.

Sample Output

show chassis alarms

`user@host>` **show chassis alarms**

```
4 alarms currently active
Alarm time               Class  Description
2012-05-29 16:47:18 UTC  Major  /var partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /var partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Major  /root partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /root partition usage crossed high threshold
```

show chassis cluster ip-monitoring status redundancy-group

Syntax

```
show chassis cluster ip-monitoring status
<redundancy-group  group-number>
```

Release Information

Command introduced in Junos OS Release 9.6. Support for global threshold, current threshold, and weight of each monitored IP address added in Junos OS Release 12.1X47-D10.

Description

Display the status of all monitored IP addresses for a redundancy group.

Options

- none— Display the status of monitored IP addresses for all redundancy groups on the node.
- **redundancy-group *group-number***— Display the status of monitored IP addresses under the specified redundancy group.

Required Privilege Level

view

RELATED DOCUMENTATION

clear chassis cluster failover-count

List of Sample Output

show chassis cluster ip-monitoring status on page 3017
show chassis cluster ip-monitoring status redundancy-group on page 3018

Output Fields

Table 280 on page 3015 lists the output fields for the **show chassis cluster ip-monitoring status** command.

Table 280: show chassis cluster ip-monitoring status Output Fields

Field Name	Field Description
Redundancy-group	ID number (0 - 255) of a redundancy group in the cluster.
Global threshold	Failover value for all IP addresses monitored by the redundancy group.

Table 280: show chassis cluster ip-monitoring status Output Fields *(continued)*

Field Name	Field Description
Current threshold	Value equal to the global threshold minus the total weight of the unreachable IP address.
IP Address	Monitored IP address in the redundancy group.
Status	Current reachability state of the monitored IP address. Values for this field are: **reachable**, **unreachable**, and **unknown**. The status is "unknown" if Packet Forwarding Engines (PFEs) are not yet up and running.
Failure count	Number of attempts to reach an IP address.
Reason	Explanation for the reported status. See Table 281 on page 3016.
Weight	Combined weight (0 - 255) assigned to all monitored IP addresses. A higher weight value indicates greater importance.

Expanded reason output fields for unreachable IP addresses added in Junos OS Release 10.1. You might see any of the following reasons displayed.

Table 281: show chassis cluster ip-monitoring status redundancy group Reason Fields

Reason	Reason Description
No route to host	The router could not resolve the ARP, which is needed to send the ICMP packet to the host with the monitored IP address.
No auxiliary IP found	The redundant Ethernet interface does not have an auxiliary IP address configured.
Reth child not up	A child interface of a redundant Ethernet interface is down.
redundancy-group state unknown	Unable to obtain the state (primary, secondary, secondary-hold, disable) of a redundancy-group.
No reth child MAC address	Could not extract the MAC address of the redundant Ethernet child interface.
Secondary link not monitored	The secondary link might be down (the secondary child interface of a redundant Ethernet interface is either down or non-functional).

Table 281: show chassis cluster ip-monitoring status redundancy group Reason Fields *(continued)*

Reason	Reason Description
Unknown	The IP address has just been configured and the router still does not know the status of this IP. or Do not know the exact reason for the failure.

Sample Output

show chassis cluster ip-monitoring status

`user@host>` **show chassis cluster ip-monitoring status**

```
node0:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address               Status        Failure count  Reason    Weight
10.254.5.44              reachable       0            n/a       220
2.2.2.1                  reachable       0            n/a       100

node1:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address               Status        Failure count  Reason    Weight
10.254.5.44              reachable       0            n/a       220
2.2.2.1                  reachable       0            n/a       100
```

Sample Output

show chassis cluster ip-monitoring status redundancy-group

`user@host>` **show chassis cluster ip-monitoring status redundancy-group 1**

```
node0:
--------------------------------------------------------------------------

Redundancy group: 1

IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a

node1:
--------------------------------------------------------------------------

Redundancy group: 1

IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a
```

show interfaces snmp-index

Syntax

```
show interfaces snmp-index snmp-index
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display information for the interface with the specified SNMP index.

Options

This command has no options.

Additional Information

Output from both the **show interfaces *interface-name* detail** and the **show interfaces *interface-name* extensive** command includes all the information displayed in the output from the **show interfaces snmp-index** command.

Required Privilege Level

view

List of Sample Output

show interfaces snmp-index on page 3019

Output Fields

The output fields from the **show interfaces snmp-index *snmp-index*** command are identical to those produced by the **show interfaces *interface-name*** command. For a description of output fields, see the other chapters in this manual.

Sample Output

show interfaces snmp-index

`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
Link flags     : Keepalives
CoS queues     : 8 supported
Last flapped   : 2005-06-15 11:45:57 PDT (05:38:43 ago)
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 summary

Syntax

```
show interfaces summary
```

Release Information

Command introduced in Junos OS Release 14.1R2.

Description

Display the status and statistics on logical interfaces configured on the device at the Flexible PIC Concentrator (FPC) level.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show interfaces summary on page 3022

Output Fields

Table 282 on page 3021 describes the output fields for the **show interfaces summary** command. Output fields are listed in the approximate order in which they appear.

Table 282: show interfaces summary Output Fields

Field Name	Field Description
System's maximum logical interfaces	Total number of logical interfaces in the device.
Logical interfaces allocated	Number of allocated logical interfaces.
Logical interfaces available	Number of available logical interfaces.
Logical interface type	The type of logical interfaces. • **LSI**—Number of label-switched logical interfaces and their status. • **Ethernet Untagged**—Number of untagged logical interfaces and their status. • **Ethernet VLAN**—Number of tagged logical interfaces and their status. • **Others**—Number of dynamic and other logical interfaces, and their status.
System	Statistics on the global logical interfaces in the system.

Table 282: show interfaces summary Output Fields *(continued)*

Field Name	Field Description
FPC x	Statistics on the logical interfaces in a specific FPC.

Sample Output

show interfaces summary

`user@host>` **show interfaces summary**

```
Logical interfaces:
    System's maximum logical interfaces  : 262144
    Logical interfaces allocated         :     31
    Logical interfaces available         : 262113

    System:
    Logical interface type    Count         UP       DOWN
    Total                        28         28          0
    LSI                           0          0          0
    Ethernet Untagged            15         15          0
    Ethernet VLAN                 0          0          0
    Others                       13         13          0

    FPC1:
    Logical interface type    Count         UP       DOWN
    Total                         3          3          0
    LSI                           0          0          0
    Ethernet Untagged             3          3          0
    Ethernet VLAN                 0          0          0
    Others                        0          0          0

    FPC2:
    Logical interface type    Count         UP       DOWN
    Total                         0          0          0
    LSI                           0          0          0
    Ethernet Untagged             0          0          0
    Ethernet VLAN                 0          0          0
    Others                        0          0          0
```

show ilmi statistics

Syntax

```
show ilmi statistics
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display input and output Integrated Local Management Interface (ILMI) statistics.

Options

This command has no options.

Required Privilege Level

view

RELATED DOCUMENTATION

clear ilmi statistics | **2965**

List of Sample Output

show ilmi statistics on page 3026

Output Fields

Table 283 on page 3024 lists the output fields for the **show ilmi statistics** command. Output fields are listed in the approximate order in which they appear.

Table 283: show ilmi statistics Output Fields

Field Name	Field Description
Input	

Table 283: show ilmi statistics Output Fields *(continued)*

Field Name	Field Description
	Information about received ILMI packets: • **Packets**—Total number of messages delivered to the ILMI entity from the transport service. • **Bad versions**—Total number of messages delivered to the ILMI entity that were for an unsupported ILMI version. • **Bad community names**—Total number of messages delivered to the ILMI entity that did not use an ILMI community name. • **Bad community uses**—Total number of messages delivered to the ILMI entity that represented an ILMI operation that was not allowed by the ILMI community named in the message. • **ASN parse errors**—Total number of ASN.1 or BER errors encountered by the ILMI entity when decoding received ILMI messages. • **Too bigs**—Total number of ILMI packets delivered to the ILMI entity with an error status field of **tooBig**. • **No such names**—Total number of ILMI packets delivered to the ILMI entity with an error status field of **noSuchName**. • **Bad values**—Total number of ILMI packets delivered to the ILMI entity with an error status field of **badValue.** • **Read onlys**—Total number of valid ILMI packets delivered to the ILMI entity with an error status field of **readOnly**. Only incorrect implementations of ILMI generate this error. • **General errors**—Total number of ILMI packets delivered to the ILMI entity with an error status field of **genErr**. • **Total request varbinds**—Total number of objects retrieved successfully by the ILMI entity as a result of receiving valid ILMI **GetRequest** and **GetNext** packets. • **Total set varbinds**—Total number of objects modified successfully by the ILMI entity as a result of receiving valid ILMI **SetRequest** packets. • **Get requests**—Total number of ILMI **GetRequest** packets that have been accepted and processed by the ILMI entity. • **Get nexts**—Total number of ILMI **GetNext** packets that have been accepted and processed by the ILMI entity. • **Set requests**—Total number of ILMI **SetRequest** packets that have been accepted and processed by the ILMI entity. • **Get responses**—Total number of ILMI **GetResponse** packets that have been accepted and processed by the ILMI entity. • **Traps**—Total number of ILMI traps received by the ILMI entity. • **Silent drops**—Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequest**, and **InformRequest** packets delivered to the ILMI entity that were silently dropped because the size of a reply containing an alternate response packet with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.

Table 283: show ilmi statistics Output Fields *(continued)*

Field Name	Field Description
	• **Proxy drops**—Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequest**, and **InformRequest** packets delivered to the ILMI entity that were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in such a way (other than a timeout) that no response packet could be returned.
Output	Information about transmitted ILMI packets: • **Packets**—Total number of messages passed from the ILMI entity to the transport service. • **Too bigs**—Total number of ILMI packets generated by the ILMI entity with an error status field of **tooBig**. • **No such names**—Total number of ILMI packets generated by the ILMI entity with an error status field of **noSuchName**. • **Bad values**—Total number of ILMI packets generated by the ILMI entity with an error status field of **badValue**. • **General errors**—Total number of ILMI packets generated by the ILMI entity with an error status field of **genErr**. • **Get requests**—Total number of ILMI **GetRequest** packets that have been generated by the ILMI entity. • **Get nexts**—Total number of ILMI **GetNext** packets that have been generated by the ILMI entity. • **Set requests**—Total number of ILMI **SetRequest** packets that have been generated by the ILMI entity. • **Get responses**—Total number of ILMI **GetResponse** packets that have been generated by the ILMI entity. • **Traps**—Total number of ILMI traps generated by the ILMI entity.

Sample Output

show ilmi statistics

```
user@host> show ilmi statistics
```

```
ILMI statistics:
 Input:
   Packets: 0, Bad versions: 0, Bad community names: 0,
   Bad community uses: 0, ASN parse errors: 0,
   Too bigs: 0, No such names: 0, Bad values: 0,
   Read onlys: 0, General errors: 0,
   Total request varbinds: 0, Total set varbinds: 0,
   Get requests: 0, Get nexts: 0, Set requests: 0,
   Get responses: 0, Traps: 0,
   Silent drops: 0, Proxy drops 0
```

```
Output:
  Packets: 0, Too bigs: 0, No such names: 0,
  Bad values: 0, General errors: 0,
  Get requests: 0, Get nexts: 0, Set requests: 0,
  Get responses: 0, Traps: 0
```

show security alarms

Syntax

```
show security alarms
<detail>
<alarm-id id-number>
<alarm-type [ types ]>
<newer-than YYYY-MM-DD.HH:MM:SS>
<older-than YYYY-MM-DD.HH:MM:SS>
<process process>
<severity severity>
```

Release Information

Command introduced in Junos OS Release 11.2.

Description

Display the alarms that are active on the device. Run this command when the CLI prompt indicates that a security alarm has been raised, as shown here:

```
[1 SECURITY ALARM] user@host#
```

Options

none—Display all active alarms.

detail—(Optional) Display detailed output.

alarm-id *id-number*—(Optional) Display the specified alarm.

alarm-type [*types*]—(Optional) Display the specified alarm type or a set of types.

You can specify one or more of the following alarm types:

- **authentication**
- **cryptographic-self-test**
- **decryption-failures**
- **encryption-failures**
- **ike-phase1-failures**
- **ike-phase2-failures**
- **key-generation-self-test**
- **non-cryptographic-self-test**

- **policy**
- **replay-attacks**

newer-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Display active alarms that were raised after the specified date and time.

older-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Display active alarms that were raised before the specified date and time.

process *process*—(Optional) Display active alarms that were raised by the specified system process.

severity *severity*—(Optional) Display active alarms of the specified severity.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

Required Privilege Level
security—To view this statement in the configuration.

RELATED DOCUMENTATION

clear security alarms

Example: Generating a Security Alarm in Response to Policy Violations

List of Sample Output
show security alarms on page 3030
show security alarms detail on page 3030
show security alarms alarm-id on page 3031
show security alarms alarm-type authentication on page 3031
show security alarms newer-than <time> on page 3032
show security alarms older-than <time> on page 3032
show security alarms process <process> on page 3032

show security alarms severity <severity> on page 3032

Output Fields

Table 284 on page 3030 lists the output fields for the **show security alarms** 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.

Table 284: show security alarms

Field Name	Field Description	Level of Output
ID	Identification number of the alarm.	All levels
Alarm time	Date and time the alarm was raised..	All levels
Message	Information about the alarm, including the alarm type, username, IP address, and port number.	All levels
Process	System process (For example, login or sshd) and process identification number associated with the alarm.	**detail**
Severity	Severity level of the alarm.	**detail**

Sample Output

show security alarms

```
[3 SECURITY ALARMS] user@router> show security alarms
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms detail

```
[3 SECURITY ALARMS] user@router> show security alarms detail
```

```
Alarm ID   : 1
Alarm Type : authentication
Time       : 2010-01-19 13:41:36 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 2
Alarm Type : authentication
Time       : 2010-01-19 13:41:52 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 3
Alarm Type : authentication
Time       : 2010-01-19 13:42:13 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice
```

show security alarms alarm-id

`[3 SECURITY ALARMS] user@router>` **show security alarms alarm-id 1**

```
ID    Alarm time              Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms alarm-type authentication

`[3 SECURITY ALARMS] user@router>` **show security alarms alarm-type authentication**

```
ID    Alarm time              Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
```

```
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms newer-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms newer-than 2010-01-19.13:41:59
```

```
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms older-than 2010-01-19.13:41:59
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> show security alarms process sshd
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms severity <severity>

```
[3 SECURITY ALARMS] user@router> show security alarms severity notice
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security datapath-debug capture

Syntax

```
show security datapath-debug capture
```

Release Information

Command introduced in Junos OS Release 10.0.

Description

Display details of the data path debugging capture file.

Required Privilege Level

view

RELATED DOCUMENTATION

show security datapath-debug counter | 3036

Understanding Data Path Debugging for Logical Systems

List of Sample Output

show security datapath—debug capture on page 3034

Output Fields

Output fields are listed in the approximate order in which they appear.

Sample Output

show security datapath—debug capture

`user@host>` **show security datapath-debug capture**

```
Packet 1, len 120: (C0/F0/P0/SEQ:71:lbt)
91 00 00 47 11 00 10 00 9a 14 00 19 03 00 00 00
00 00 00 00 00 01 00 47 10 00 00 00 00 00 00 00
00 1f 12 f8 dd 29 00 21 59 84 f4 01 81 00 02 1e
08 00 45 60 01 f4 00 00 00 00 3f 06 73 9f 01 01
01 02 03 01 01 02 d4 31 d4 31 00 00 00 00 00 00
00 00 50 02 00 00 ff ad 00 00 00 00
Packet 2, len 120: (C0/F0/P0/SEQ:71:lbt)
90 00 00 47 04 00 00 00 00 00 00 00 02 02 00 47
```

```
10 00 00 00 00 00 00 00 50 00 a6 1c 00 00 00 00
00 00 00 0a 00 00 00 00 00 00 09 d9 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 1f 12 f8
dd 29 00 21 59 84 f4 01 81 00 02 1e
```

show security datapath-debug counter

Syntax

```
show security datapath-debug counter
```

Release Information

Command introduced in Junos OS Release 10.0.

Description

Display details of the data path debugging counter.

Required Privilege Level

view

RELATED DOCUMENTATION

show security datapath-debug capture | 3034

Understanding Data Path Debugging for Logical Systems

List of Sample Output

show security datapath-debug counter on page 3036

Output Fields

Output fields are listed in the approximate order in which they appear.

Sample Output

show security datapath-debug counter

`user@host>` **show security datapath-debug counter**

```
Datapath debug counters
Packet Filter 1:
np-ingress
Chassis 0 FPC 4 : 1
np-ingress
Chassis 0 FPC 3 : 0
np-egress
Chassis 0 FPC 4 : 1
np-egress
```

```
Chassis 0 FPC 3 : 0
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 2
pot
Chassis 0 FPC 0 PIC 1: 0
pot
```

show security monitoring

Syntax

```
show security monitoring
```

Release Information

Command introduced in Junos OS Release 10.2.

Description

Displays a count of security flow and central point (CP) sessions, CPU utilization (as a percentage of maximum), and memory in use (also as a percentage of maximum) at the moment the command is run. This command is supported on SRX1400, SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Required Privilege Level

View

RELATED DOCUMENTATION

- show security monitoring fpc fpc-number | 3041
- show security monitoring performance session | 3045
- show security monitoring performance spu | 3047

show security monitoring

user@host>show security monitoring

```
user@host> show security monitoring
-------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem         current        maximum        current        maximum
-------------------------------------------------------------------------
  1   0   0  11               0              0              0              0
  1   1   0   5               3        6291456              1        7549747
  1   2   0   5               2        6291456              0        7549747
  1   3   0   5               3        6291456              1        7549747
  8   0   0  65               4           6963              2           8355
  8   1   0  65               2           6963              0           8355
```

```
Total Sessions:             14       18888294             4       22665951
```

show security monitoring (SRX1400)

user@host>show security monitoring

```
user@host> show security monitoring
-------------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem        current        maximum        current        maximum
-------------------------------------------------------------------------------
  1   0   0  75              0        1048576            0          1048576
```

show security monitoring (vSRX)

user@host>show security monitoring

```
user@host> show security monitoring
-------------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem        current        maximum        current        maximum
-------------------------------------------------------------------------------
  0   0   0  68              2         524288            N/A            N/A
```

show security monitoring (vSRX in a Chassis Cluster)

user@host>show security monitoring

```
node0:
--------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem        current        maximum        current        maximum
--------------------------------------------------------------------------
```

```
  0   0   0  67              0         524288            N/A            N/A

node1:
--------------------------------------------------------------------------
                  Flow session   Flow session     CP session     CP session
FPC PIC CPU Mem         current        maximum        current        maximum
--------------------------------------------------------------------------
  0   0   0  67              0         524288            N/A            N/A
```

show security monitoring fpc fpc-number

Syntax

show security monitoring fpc ***fpc-number***
<node (***node-id*** | all | local | primary)>

Release Information

Command introduced in Junos OS Release 9.2.

Description

Display security monitoring information about the FPC slot.

Options

- ***fpc-number*** —Display security monitoring information for the specified FPC slot. It can be in the range from 0 to 11.
- **node**—(Optional) For chassis cluster configurations, display security monitoring information for the specified FPC on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

Additional Information

For complete list of slot numbering, physical port, and logical interface numbering for SRX Series devices in chassis cluster, see *Chassis Cluster User Guide for SRX Series Devices*.

Required Privilege Level

view

RELATED DOCUMENTATION

show services ip-monitoring status | 3051

List of Sample Output

show security monitoring fpc 0 on page 3042
show security monitoring fpc 1 on page 3043
show security monitoring fpc 8 on page 3043

Output Fields

Table 285 on page 3042 lists the output fields for the **show security monitoring fpc *fpc-number*** command. Output fields are listed in the approximate order in which they appear.

Table 285: show security monitoring fpc fpc-number Output Fields

Field Name	Field Description
FPC	Slot number in which the FPC is installed.
PIC	Slot number in which the PIC is installed.
CPU Utilization (%)	Total percentage of CPU being used by the PIC's processors.
Memory Utilization (%)	Percentage of heap space (dynamic memory) being used by the PIC's processor. If this number exceeds 80 percent, there might be a software problem (memory leak).
Current flow session	The current number of flow sessions. When SRX Series devices operate in packet mode, flow sessions will not be created and this field will remain zero.
Max flow session	The maximum number of flow sessions allowed. This number will differ from one device to another.
SPU current cp session	The current number of cp sessions for the SPU (on SRX5600, and SRX5800 devices only).
SPU max cp session	The maximum number of cp sessions allowed for the SPU (on SRX5600, and SRX5800 devices only).

Sample Output

show security monitoring fpc 0

```
user@host> show security monitoring fpc 0
```

```
FPC 0
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   82 %
    Current flow session :    0
    Max flow session     :    0
    Current CP session   :    0
    Max CP session       : 12000000
```

```
Session Creation Per Second (for last 96 seconds on average):    0
  PIC 1
    CPU utilization      :    0 %
    Memory utilization   :   54 %
    Current flow session :    0
    Max flow session     : 819200
    Current CP session   :    0
    Max CP session       :    0
Session Creation Per Second (for last 96 seconds on average):    0
```

Sample Output

show security monitoring fpc 1

user@host> **show security monitoring fpc 1**

```
FPC 1
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   21 %
    Current flow session :    0
    Max flow session     : 524288
    Current CP session   :    0
    Max CP session       : 1048576
Session Creation Per Second (for last 96 seconds on average):    0
```

Sample Output

show security monitoring fpc 8

user@host> **show security monitoring fpc 5**

```
FPC 5
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   64 %
    Current flow session :    0
    Max flow session     : 524288
    Current CP session   :    0
```

```
    Max CP session       : 2359296
Session Creation Per Second (for last 96 seconds on average):    0
  PIC 1
    CPU utilization      :    0 %
    Memory utilization   :   65 %
    Current flow session :    0
    Max flow session     : 1048576
    Current CP session   :    0
    Max CP session       :    0
Session Creation Per Second (for last 96 seconds on average):    0
```

show security monitoring performance session

Syntax

```
show security monitoring performance session

       <fpc slot-number>

       <pic slot-number>
```

Release Information

Command introduced in Junos OS Release of 10.2.

Description

Display the current session (total number of sessions at that time) for the last 60 seconds.

Options

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.

> **NOTE:** The fpc slot-number and pic slot-number options are not available on SRX300, SRX320, and SRX340 devices.

Required Privilege Level

View

RELATED DOCUMENTATION

show services ip-monitoring status | 3051

show security monitoring performance session

user@host> show security monitoring performance session

```
fpc  0  pic  0
Last 60 seconds:
 0:       8   1:       8   2:       8   3:       8   4:       8   5:       7
 6:       7   7:       7   8:       7   9:       7  10:       7  11:       8
12:       8  13:       8  14:       7  15:       7  16:       7  17:       7
18:       7  19:       7  20:       7  21:       5  22:       5  23:       5
24:       5  25:       5  26:       5  27:       5  28:       5  29:       4
30:       4  31:       4  32:       3  33:       3  34:       3  35:       3
36:       5  37:       5  38:       6  39:       6  40:       5  41:       5
42:       5  43:       5  44:       5  45:       5  46:       5  47:       5
48:       7  49:       7  50:       6  51:       8  52:       8  53:       6
54:       5  55:       7  56:       7  57:       5  58:       5  59:       8
```

show security monitoring performance spu

Syntax

```
show security monitoring performance spu

       <fpc slot-number>

       <pic slot-number>
```

Release Information
Command introduced in Junos OS Release 10.2.

Description

Display the services processing unit (SPU) percent utilization for all FPC slots over the last 60 seconds. Use this command to track the percent utilization statistics per second for the past 60 seconds for each FPC slot and PIC.

Starting in Junos OS Release 20.2R1, you can use the following operational commands to monitor the average CPU usage information for the last minute, hour, or day of an SPC3 card:

- **show security monitoring performance spu summary fpc *fpc-slot-number* pic *pic-slot-number***
- **show security monitoring performance spu summary fpc *fpc-slot-number* pic *pic-slot-number* thread *thread-number***

You can monitor the CPU usage information only when the PIC is online.

Options

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.

> **NOTE:** The fpc slot-number and pic slot-number options are not available on SRX300, SRX320, or SRX340 devices or on vSRX instances.

Required Privilege Level
View

RELATED DOCUMENTATION

show services ip-monitoring status | 3051

show security monitoring performance spu

This sample shows 46% utilization of the SPU for second 42 in the past 60 seconds for FPC 0 and PIC 0.

user@host> show security monitoring performance spu

```
fpc  0  pic  0
Last 60 seconds:
 0:  48   1:  48   2:  48   3:  48   4:  48   5:  48
 6:  48   7:  48   8:  49   9:  48  10:  48  11:  48
12:  48  13:  48  14:  48  15:  48  16:  48  17:  48
18:  48  19:  48  20:  48  21:  48  22:  49  23:  48
24:  49  25:  49  26:  48  27:  48  28:  48  29:  48
30:  48  31:  48  32:  48  33:  48  34:  48  35:  48
36:  46  37:  47  38:  46  39:  46  40:  46  41:  46
42:  46  43:  46  44:  46  45:  46  46:  46  47:  46
48:  46  49:  46  50:  46  51:  46  52:  46  53:  46
54:  46  55:  46  56:  46  57:  46  58:  46  59:  46
```

show security monitoring performance spu (vSRX and vSRX 3.0)

user@host> show security monitoring performance spu

```
fpc  0  pic  0
Last 60 seconds:
  0:    0    1:   0    2:    0    3:    0    4:    0    5:    0
  6:    0    7:   0    8:    0    9:    0   10:    0   11:    0
 12:    0   13:   0   14:    0   15:    0   16:    0   17:    0
 18:    0   19:   0   20:    0   21:    0   22:    0   23:    0
 24:    0   25:   0   26:    0   27:    0   28:    0   29:    0
 30:    0   31:   0   32:    0   33:    0   34:    0   35:    0
 36:    0   37:   0   38:    0   39:    0   40:    0   41:    0
 42:    0   43:   0   44:    0   45:    0   46:    0   47:    0
```

```
 48:    0   49:   0   50:    0   51:    0   52:    0   53:    0
 54:    0   55:   0   56:    0   57:    0   58:    0   59:    0
```

show security monitoring performance spu summary fpc 1 pic 0 (SRX5400, SRX5600, and SRX5800)

user@host> show security monitoring performance spu summary fpc 1 pic 0

```
FPC 1 PIC 0THREAD 0
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0

THREAD 1
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0

THREAD 2
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0

... ...

THREAD 23
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0

THREAD 24
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0

THREAD 25
Last Minute Average %: 0
Last Hour Average %: 0
Last Day Average %: 0
```

show security monitoring performance spu summary fpc 1 pic 1 thread 8 (SRX5400, SRX5600, and SRX5800)

user@host> show security monitoring performance spu summary fpc 1 pic 1 thread 8

```
FPC 1 PIC 1
THREAD 8
Last Minute Average %: 0
Last Hour Average %: 5
Last Day Average %: 4
```

show services ip-monitoring status

Syntax

```
show services ip-monitoring status
```

Release Information

Command modified in Junos OS Release 11.4 R2. Next-hop functionality added in Junos OS Release 12.1X46-D15.

Description

Display a brief summary of IP monitoring status along with the current state for a given policy.

Required Privilege Level

view

RELATED DOCUMENTATION

show security monitoring | 3038

List of Sample Output

show services ip-monitoring status on page 3052
show services ip-monitoring status on page 3053
show services ip-monitoring status on page 3054
show services ip-monitoring status on page 3054
show services ip-monitoring status on page 3055
show services ip-monitoring status on page 3055

Output Fields

Table 286 on page 3051 lists the output fields for the **show services ip-monitoring status** command. Output fields are listed in the approximate order in which they appear.

Table 286: show services ip-monitoring status Output Fields

Field Name	Field Description
Policy	Name of the policy configured.
Probe Name	Name of the probe configured.
Address	Displays the configured target address.

Table 286: show services ip-monitoring status Output Fields *(continued)*

Field Name	Field Description
Status	Displays the status of the probe on the target address. If the status is PASS, then the target address is reached.
Route-Action	Displays route injection information configured for the policy and its failover status.
Route-Instance	Displays the routing instance of the route to be injected during failover.
Route	Routing address of the route to be injected during failover.
Next-Hop	Specifies the next-hop address of the route to be injected during failover. P2P interfaces only.
State	Display the state of the route injection action. If the state is APPLIED, then the ip-monitoring policy is in failover state.
Interface Action	Displays the interface action type as enable or disable.
Policy Action	Displays the policy action type as enable or disable.
Admin State	Displays the current admin state of the interface.
Action Status	Displays the current action status of the interface.

Sample Output

show services ip-monitoring status

`user@host>` **show services ip-monitoring status**

```
Policy - policy1 (Non-preemptive. Status: FAIL)
  RPM Probes:
    Probe name             Test Name       Address          Status
    ---------------------- --------------- ---------------- ---------
    probe_a                a1              15.1.1.10        FAIL
    probe_a                a2              200.1.1.1        FAIL
  Route-Action:
    route-instance    route             next-hop         State
    ----------------- ----------------- ---------------- -------------
```

```
    inet.0            200.1.1.0         150.1.1.1        APPLIED
  Interface-Action:
    interface         policy action   admin state action status
    ----------------- --------------- ----------- -----------------
    fe-0/0/5.2        Enable          UP          FAILOVER
    fe-0/0/5.4        Disable         DOWN        FAILOVER
    t1-1/0/0          Enable          UP          FAILOVER
    dl0               Enable          UP          FAILOVER
    ge-0/0/1          Enable          UP          FAILOVER
```

Sample Output

show services ip-monitoring status

In this example, the policy is in the failback state, and the no-preempt option is not configured.

`user@host>` **show services ip-monitoring status**

```
Policy - policy1 (Status: PASS)
  RPM Probes:
    Probe name             Test Name       Address          Status
    ---------------------- --------------- ---------------- ---------
    probe1                 a1              99.1.1.2         PASS
  Route-Action:
    route-instance    route             next-hop         state
    ----------------- ----------------- ---------------- -------------
    inet.0            99.1.1.0          12.12.12.2       NOT-APPLIED
  Interface-Action:
    interface         policy action   admin state action status
    ----------------- --------------- ----------- -----------------
    at-2/0/0          Enable          DOWN        MARKED-DOWN
    ge-0/0/2.2        Enable          DOWN        MARKED-DOWN
    ge-0/0/2.3        Enable          DOWN        MARKED-DOWN
```

Sample Output

show services ip-monitoring status

In this example, the policy is in the failover state, and the primary is restored. The no-preempt option is configured.

`user@host>` **show services ip-monitoring status**

```
Policy - policy1 (Non-preemptive. Status: FAILOVER-NO-PREEMPT)
  RPM Probes:
     Probe name             Test Name       Address          Status
    --------------------- -------------- --------------- ---------
     probe1                 a1              99.1.1.2         PASS
  Route-Action:
    route-instance    route             next-hop         state
    ----------------- ----------------- --------------- -------------
    inet.0            99.1.1.0          12.12.12.2       APPLIED
  Interface-Action:
    interface         policy action   admin state action status
    ----------------- -------------- ----------- -----------------
    at-2/0/0          Enable          UP          FAILOVER
    ge-0/0/2.2        Enable          UP          FAILOVER
    ge-0/0/2.3        Enable          UP          FAILOVER
```

Sample Output

show services ip-monitoring status

When the probe succeeds and the policy is not applied, the output is as follows:

`user@host>` **show services ip-monitoring status**

```
Policy payment (Status: PASS)
 RPM Probes:
     Probe name             Test Name       Address          Status
    --------------------- -------------- --------------- ---------
     Probe-Payment-Server   paysvr          9.9.9.2          PASS
 Route-Action:
    route-instance    route             next-hop         state
    ----------------- ----------------- --------------- -------------
    inet.0            9.9.9.0/24        e1-6/0/0.0       NOT-APPLIED
```

Sample Output

show services ip-monitoring status

When the probe fails and the policy is applied, the output is as follows:

`user@host>` **show services ip-monitoring status**

```
Policy payment (Status: FAIL)
 RPM Probes:
     Probe name             Test Name       Address          Status
    ---------------------- -------------- ---------------- ---------
     Probe-Payment-Server   paysvr          9.9.9.2          FAIL
 Route-Action:
    route-instance    route             next-hop         state
    ----------------- ----------------- ---------------- -------------
    inet.0            9.9.9.0/24        e1-6/0/0.0       APPLIED
```

Sample Output

show services ip-monitoring status

When the probe fails and the policy is applied, the output is as follows. The status of the route **WITHDRAWED** indicates that this route is removed.

`user@host>` **show services ip-monitoring status**

```
Policy - p1 (Status: FAIL)
  RPM Probes:
    Probe name             Test Name       Address          Status
    ---------------------- -------------- ---------------- ---------
    p1                     t1              200.20.2.2       FAIL
  Route-Action:
    route-instance    route             next-hop         state
    ----------------- ----------------- ---------------- -------------
     inet.0         111.111.111.1/32   10.208.128.1     WITHDRAWED
```

show services rpm twamp client connection

Syntax

```
show services rpm twamp client connection
<connection-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display information about the connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default, all established sessions are displayed, unless you specify a control connection name when you issue the command.

Options

connection-name—(Optional) Display information about the specified control connection or TWAMP control client.

Required Privilege Level

view

List of Sample Output

show services rpm twamp client connection on page 3057

Output Fields

Table 287 on page 3056 lists the output fields for the **show services rpm twamp client connection** command. Output fields are listed in the approximate order in which they appear.

Table 287: show services rpm twamp client connection Output Fields

Field Name	Field Description
Connection Name	Connection name that uniquely identifies the connection between the TWAMP server and a particular client.
Client address	Client IP address.
Client port	Client port number.
Server address	Server IP address.
Server port	Server port number.

Table 287: show services rpm twamp client connection Output Fields *(continued)*

Field Name	Field Description
Session count	Session count.
Auth mode	Authentication mode.

Sample Output

show services rpm twamp client connection

`user@host>` **show services rpm twamp client connection**

```
Connection      Client          Client Server          Server Session Auth
Name            address         port   address         port   count   mode
c1              123.0.0.2        60530 123.0.0.1         1862       1
Unauthenticated
```

show services rpm twamp client history-results

Syntax

```
show services rpm history-results
<brief | detail>
<control-connection control-connection-name>
<since time>
<test-session test-session-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) instance. You can also view the historical results of the probes or test packets sent from a TWAMP client to a TWAMP server for a particular control connection, or a test session associated with a control connection.

Options

brief | detail—(Optional) Display the specified level of output.

control-connection *control-connection-name*—(Optional) Display information for the specified control connection between a TWAMP client and a TWAMP server.

since *time*—(Optional) Display information from the specified time. Specify time as ***yyyy-mm-dd.hh:mm:ss***.

test-session *test-session-name*—(Optional) Display information for the specified test session associated with a control connection between a TWAMP client and a TWAMP server.

Required Privilege Level

view

List of Sample Output

show services rpm twamp client history-results on page 3059

Output Fields

Table 218 on page 2597 lists the output fields for the **show services rpm twamp client history-results** command. Output fields are listed in the approximate order in which they appear.

Table 288: show services rpm twamp client history-results Output Fields

Field Name	Field Description
Owner	Probe owner or the TWAMP client.

Table 288: show services rpm twamp client history-results Output Fields *(continued)*

Field Name	Field Description
Test	Name of a test for a TWAMP probe instance.
Probe received	Timestamp when the probe result was received.
Round trip time	Average ping round-trip time (RTT), in microseconds.
Probes sent	Timestamp when the probe result was sent.
Round trip time	Average ping RTT, in microseconds.

Sample Output

show services rpm twamp client history-results

`user@host>` **show services rpm twamp client history-results**

```
Owner, Test                Probe Sent              Probe received
Round trip time
    c2, t2                     Fri Jul 21 05:11:06 2017 Fri Jul 21 05:11:06 2017
              241 usec
    c2, t2                     Fri Jul 21 05:11:07 2017 Fri Jul 21 05:11:07 2017
              254 usec
    c2, t2                     Fri Jul 21 05:11:08 2017 Fri Jul 21 05:11:08 2017
              248 usec
    c2, t2                     Fri Jul 21 05:11:09 2017 Fri Jul 21 05:11:09 2017
              241 usec
    c2, t2                     Fri Jul 21 05:11:10 2017 Fri Jul 21 05:11:10 2017
              245 usec
    c2, t2                     Fri Jul 21 05:11:11 2017 Fri Jul 21 05:11:11 2017
              231 usec
    c2, t2                     Fri Jul 21 05:11:12 2017 Fri Jul 21 05:11:12 2017
              258 usec
    c2, t2                     Fri Jul 21 05:11:13 2017 Fri Jul 21 05:11:13 2017
              232 usec
    c2, t2                     Fri Jul 21 05:11:14 2017 Fri Jul 21 05:11:14 2017
              236 usec
    c2, t2                     Fri Jul 21 05:11:15 2017 Fri Jul 21 05:11:15 2017
              236 usec
```

```
    c2, t2                      Fri Jul 21 05:11:16 2017 Fri Jul 21 05:11:16 2017
              213 usec
```

show services rpm twamp client probe-results

Syntax

```
show services rpm twamp client probe-results
<control-connection control-connection-name>
<test-session test-session-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display the results of the most recent real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) probes sent from the TWAMP client to the TWAMP server. You can also view the results of the probes or test packets sent from a TWAMP client to a TWAMP server for a particular control connection, or a test session associated with a control connection.

Options

control-connection *control-connection-name*—(Optional) Display information for the specified control connection between a TWAMP client and a TWAMP server.

test-session *test-session-name*—(Optional) Display information for the specified test session associated with a control connection between a TWAMP client and a TWAMP server.

Required Privilege Level

view

List of Sample Output

show services rpm twamp client probe-results on page 3065

Output Fields

Table 289 on page 3061 lists the output fields for the **show services twamp client probe-results** command. Output fields are listed in the approximate order in which they appear.

Table 289: show services twamp client probe-results Output Fields

Field Name	Field Description
Owner	Name of the session-sender or the control client, which is the TWAMP client. When you configure the ***control-client-name*** option at the **[edit services twamp client control-connection]** hierarchy level, this field displays the configured owner name or the client name.
Test	Name of a test representing a collection of probes. When you configure the **test-session *test-name*** statement at the **[edit services owner]** hierarchy level, the field displays the configured test name.

Table 289: show services twamp client probe-results Output Fields *(continued)*

Field Name	Field Description
server-address	Destination address used for the probes.
server-port	Destination port used for the probes.
Client address	Source or TWAMP client address used for the probes.
Client port	Source or TWAMP client port used for the probes.
Reflector address	Session reflector or TWAMP server address used for the probes.
Reflector port	Session reflector or TWAMP server port used for the probes.
Test size	Number of probes within a test.
Probe results	Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement: • **Response received**—Timestamp when the probe result was determined. • **Client and server hardware timestamps**—If timestamps are configured, an entry appears at this point. • **Rtt**—Average ping round-trip time (RTT), in microseconds. • **Egress jitter**—Egress jitter, in microseconds. • **Ingress jitter**—Ingress jitter, in microseconds. • **Round trip jitter**—Round-trip jitter, in microseconds. • **Egress interarrival jitter**—Egress interarrival jitter, in microseconds. • **Ingress interarrival jitter**—Ingress interarrival jitter, in microseconds. • **Round trip interarrival jitter**—Round-trip interarrival jitter, in microseconds.

Table 289: show services twamp client probe-results Output Fields *(continued)*

Field Name	Field Description
Results over current test	Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes. • **Probes sent**—Number of probes sent within the current test. • **Probes received**—Number of probe responses received within the current test. • **Loss percentage**—Percentage of lost probes for the current test. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individual calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.

Table 289: show services twamp client probe-results Output Fields *(continued)*

Field Name	Field Description
Results over last test	Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed: • **Probes sent**—Number of probes sent for the most recently completed test. • **Probes received**—Number of probe responses received for the most recently completed test. • **Loss percentage**—Percentage of lost probes for the most recently completed test. • **Test completed**—Time the most recent test was completed. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individually calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured for the most recently completed test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.

Table 289: show services twamp client probe-results Output Fields *(continued)*

Field Name	Field Description
Results over all tests	Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test. • **Probes sent**—Number of probes sent in all tests. • **Probes received**—Number of probe responses received in all tests. • **Loss percentage**—Percentage of lost probes in all tests. • **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types **icmp-ping-timestamp** and **udp-ping-timestamp**, the egress delay and ingress delay. For each measurement type, the following individually calculated results are provided: ◦ **Samples**—Number of probes. ◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test. ◦ **Peak to peak**—Peak-to-peak difference, in microseconds. ◦ **Stddev**—Standard deviation, in microseconds. ◦ **Sum**—Statistical sum.

Sample Output

show services rpm twamp client probe-results

`user@host>` **show services rpm twamp client probe-results**

```
Owner: c2, Test: t2
    server-address: 23.0.0.1, server-port: 862, Client address: 23.0.0.1,
    Client port: 63223
    Reflector address: 23.0.0.1, Reflector port: 10000,
    Sender address: 23.0.0.1, sender-port: 10000
    Test size: 400000 probes
    Probe results:
      Response received
      Fri Jul 21 05:12:12 2017
```

```
      Fri Jul 21 05:12:12 2017
      Rtt: 242 usec, Egress jitter: -9 usec, Ingress jitter: 24 usec,
      Round trip jitter: 15 usec, Egress interarrival jitter: 14 usec,
      Ingress interarrival jitter: 18 usec,
      Round trip interarrival jitter: 16 usec
    Results over current test:
      Probes sent: 67, Probes received: 67, Loss percentage: 0.000000
      Measurement: Round trip time
Samples: 67, Minimum: 206 usec, Maximum: 266 usec, Average: 243 usec,
        Peak to peak: 60 usec, Stddev: 11 usec, Sum: 16283 usec
      Measurement: Negative egress jitter
        Samples: 66, Minimum: 4 usec, Maximum: 25 usec, Average: 14 usec,
        Peak to peak: 21 usec, Stddev: 4 usec, Sum: 935 usec
      Measurement: Positive ingress jitter
        Samples: 55, Minimum: 0 usec, Maximum: 62 usec, Average: 19 usec,
        Peak to peak: 62 usec, Stddev: 13 usec, Sum: 1023 usec
      Measurement: Negative ingress jitter
        Samples: 11, Minimum: 1 usec, Maximum: 23 usec, Average: 8 usec,
        Peak to peak: 22 usec, Stddev: 6 usec, Sum: 87 usec
      Measurement: Positive round trip jitter
        Samples: 33, Minimum: 0 usec, Maximum: 49 usec, Average: 14 usec,
        Peak to peak: 49 usec, Stddev: 11 usec, Sum: 463 usec
      Measurement: Negative round trip jitter
        Samples: 33, Minimum: 1 usec, Maximum: 34 usec, Average: 14 usec,
        Peak to peak: 33 usec, Stddev: 8 usec, Sum: 462 usec
    Results over all tests:
      Probes sent: 67, Probes received: 67, Loss percentage: 0.000000
      Measurement: Round trip time
        Samples: 67, Minimum: 206 usec, Maximum: 266 usec, Average: 243 usec,
        Peak to peak: 60 usec, Stddev: 11 usec, Sum: 16283 usec
      Measurement: Negative egress jitter
        Samples: 66, Minimum: 4 usec, Maximum: 25 usec, Average: 14 usec,
        Peak to peak: 21 usec, Stddev: 4 usec, Sum: 935 usec
      Measurement: Positive ingress jitter
        Samples: 55, Minimum: 0 usec, Maximum: 62 usec, Average: 19 usec,
        Peak to peak: 62 usec, Stddev: 13 usec, Sum: 1023 usec
      Measurement: Negative ingress jitter
        Samples: 11, Minimum: 1 usec, Maximum: 23 usec, Average: 8 usec,
Peak to peak: 22 usec, Stddev: 6 usec, Sum: 87 usec
      Measurement: Positive round trip jitter
        Samples: 33, Minimum: 0 usec, Maximum: 49 usec, Average: 14 usec,
        Peak to peak: 49 usec, Stddev: 11 usec, Sum: 463 usec
      Measurement: Negative round trip jitter
```

```
Samples: 33, Minimum: 1 usec, Maximum: 34 usec, Average: 14 usec,
Peak to peak: 33 usec, Stddev: 8 usec, Sum: 462 usec
```

show services rpm twamp client session

Syntax

```
show services rpm twamp client session
<control-connection control-connection-name>
<test-session test-session-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display information about the sessions established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients for control packets and data packets. By default, all established control connection and data connection or test sessions are displayed, unless you specify a control connection name or a test session name when you issue the command.

Options

control-connection *control-connection-name*—(Optional) Display information about the specified control connection, which is established for control packets exchanged between a TWAMP client and a TWAMP server.

test-session *test-session-name*—(Optional) Display information about the specified test session, which is established for data packets transmitted between a TWAMP client and a TWAMP server, associated with a control connection.

Required Privilege Level

view

List of Sample Output

show services rpm twamp client session on page 3069

Output Fields

Table 290 on page 3068 lists the output fields for the **show services rpm twamp client session** command. Output fields are listed in the approximate order in which they appear.

Table 290: show services rpm twamp client session Output Fields

Field Name	Field Description
Connection Name	Name of the control connection that uniquely identifies the connection between the TWAMP server and the TWAMP client.
Session Name	Name of the test session that uniquely identifies the data session between the TWAMP server and the TWAMP client.

Table 290: show services rpm twamp client session Output Fields *(continued)*

Field Name	Field Description
Sender address	Sender IP address.
Sender port	Sender port number.
Reflector address	Reflector IP address.
Reflector port	Reflector port number.

Sample Output

show services rpm twamp client session

`user@host>` **show services rpm twamp client session**

```
root> show services rpm twamp client session
Connection      Session         Sender          Sender Reflector        Reflector
Name            Name            address          port   address          port
c1              t1              123.0.0.2         10001 123.0.0.1         10001
```

show services rpm twamp server connection

Syntax

```
show services rpm twamp server connection
<connection-id>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display information about the connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default, all established sessions are displayed, unless you specify a session ID when you issue the command.

Options

connection-id—(Optional) Identifier of the connection that you want to display information about.

Required Privilege Level

view

List of Sample Output

show services rpm twamp server connection on page 3071

Output Fields

Table 287 on page 3056 lists the output fields for the **show services rpm twamp server connection** command. Output fields are listed in the approximate order in which they appear.

Table 291: show services rpm twamp server connection Output Fields

Field Name	Field Description
Connection ID	Connection ID that uniquely identifies the connection between the TWAMP server and a particular client.
Client address	Client IP address.
Client port	Client port number.
Server address	Server IP address.
Server port	Server port number.
Session count	Session count.

Table 291: show services rpm twamp server connection Output Fields *(continued)*

Field Name	Field Description
Auth mode	Authentication mode.

Sample Output

show services rpm twamp server connection

`user@host>` **show services rpm twamp server connection**

```
Connection  Client           Client  Server           Server   Session  Auth
ID          address          port    address          port     count    mode
         5  123.0.0.1         50821  123.0.0.2           862         1
Unauthenticated
```

show services rpm twamp server session

Syntax

```
show services rpm twamp server session
<session-id>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D110 for SRX Series devices.

Description

Display information about the sessions established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default, all established sessions are displayed, unless you specify a session ID when you issue the command.

Options

session-id—(Optional) Identifier of the session that you want to display information about.

Required Privilege Level

view

List of Sample Output

show services rpm twamp server session on page 3073

Output Fields

Table 292 on page 3072 lists the output fields for the **show services rpm twamp server session** command. Output fields are listed in the approximate order in which they appear.

Table 292: show services rpm twamp server session Output Fields

Field Name	Field Description
Session ID	Session ID that uniquely identifies the session between the TWAMP server and a particular client.
Connection ID	Connection ID that uniquely identifies the connection between the TWAMP server and a particular client.
Sender address	Sender IP address.
Sender port	Sender port number.
Reflector address	Reflector IP address.
Reflector port	Reflector port number.

Sample Output

show services rpm twamp server session

user@host> **show services rpm twamp server session**

```
Session  Connection  Sender           Sender  Reflector        Reflector
ID       ID          address          port    address          port
      3           6  123.0.0.1         40000  123.0.0.2           40000
```

show snmp health-monitor

Syntax

```
show snmp health-monitor
<alarms <detail>> | <logs>
```

Release Information

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.

Options

none—Display information about all health monitor alarms and logs.

alarms <detail>—(Optional) Display detailed information about health monitor alarms.

logs—(Optional) Display information about health monitor logs.

Required Privilege Level

view

List of Sample Output

show snmp health-monitor on page 3076
show snmp health-monitor alarms detail on page 3079

Output Fields

Table 260 on page 2870 describes the output fields for the **show snmp health-monitor** command. Output fields are listed in the approximate order in which they appear.

Table 293: show snmp health-monitor Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
Variable description	Description of the health monitor object instance being monitored.	All levels
Variable name	Name of the health monitor object instance being monitored.	All levels
Value	Current value of the monitored variable in the most recent sample interval.	All levels

Table 293: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output

State	State of the alarm or event entry:
	• Alarms:
	  • **active**—Entry is fully configured and activated.
	  • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit.
	  • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit.
	  • **under creation**—Entry is being configured and is not yet activated.
	  • **startup**—Alarm is waiting for the first sample of the monitored variable.
	  • **object not available**—Monitored variable of that type is not available to the health monitor agent.
	  • **instance not available**—Monitored variable's instance is not available to the health monitor agent.
	  • **object type invalid**—Monitored variable is not a numeric value.
	  • **object processing errored**—An error occurred when the monitored variable was processed.
	  • **unknown**—State is not one of the above.
		All levels

Variable OID	Object ID to which the variable name is resolved. The format is **x.x.x.x**.	**detail**
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**.	**detail**

Table 293: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.
	• Alarm is *not* sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.
	  ◦ Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	**detail**
Creator	Mechanism by which the entry was configured (**Health Monitor**).	**detail**
Sample interval	Time period between samples (in seconds).	**detail**
Rising threshold	Upper limit threshold value as a percentage of the maximum possible value.	**detail**
Falling threshold	Lower limit threshold value as a percentage of the maximum possible value.	**detail**
Rising event index	Event triggered when the rising threshold is crossed.	**detail**
Falling event index	Event triggered when the falling threshold is crossed.	**detail**

Sample Output

show snmp health-monitor

```
user@host> show snmp health-monitor
```

```
Alarm
Index  Variable description                            Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                         58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                          0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                            0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                        35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                        0 active
       Chassis daemon                                    50 active
       Firewall daemon                                    0 active
       Interface daemon                                   5 active
       SNMP daemon                                       11 active
       MIB2 daemon                                       42 active
       Sonet APS daemon                                   0 active
       VRRP daemon                                        0 active
       Alarm daemon                                       3 active
       PFE daemon                                         0 active
       CRAFT daemon                                       0 active
       Traffic sampling control daemon                    0 active
       Ilmi daemon                                        0 active
       Remote operations daemon                           0 active
       CoS daemon                                         0 active
       Pic Services Logging daemon                        0 active
       Internal Routing Service Daemon                    3 active
       Network Access Service daemon                      0 active
       Forwarding UDP daemon                              0 active
       Routing socket proxy daemon                        0 active
       Disk Monitoring daemon                             1 active
       Inet daemon                                        0 active
       Syslog daemon                                      0 active
       Adaptive Services PIC daemon                       0 active
       ECC parity errors logging Daemon                   0 active
       Layer 2 Tunneling Protocol daemon                  0 active
       PPPoE daemon                                       3 active
```

```
      Redundancy device daemon                              0 active
      PPP daemon                                            0 active
      Dynamic Flow Capture Daemon                           0 active

32776 Health Monitor: jroute daemon CPU utilization
      Routing protocol daemon                               1 active
      Management daemon                                     0 active
      Management daemon                                     0 active
      Command line interface                                4 active
      Periodic Packet Management daemon                     0 active
      Link Management daemon                                0 active
      Pragmatic General Multicast daemon                    0 active
      Bidirectional Forwarding Detection daemon             0 active
      SRC daemon                                            0 active
      audit daemon                                          0 active
      Event daemon                                          0 active

32777 Health Monitor: jcrypto daemon CPU utilization
      IPSec Key Management daemon                           0 active

32779 Health Monitor: jkernel daemon Memory utilization
      Init daemon                                       47384 active
      Chassis daemon                                    20204 active
      Firewall daemon                                    1956 active
      Interface daemon                                   3340 active
      SNMP daemon                                        4540 active
      MIB2 daemon                                        3880 active
      Sonet APS daemon                                   2632 active
      VRRP daemon                                        2672 active
      Alarm daemon                                       1856 active
      PFE daemon                                         2600 active
      CRAFT daemon                                       2000 active
      Traffic sampling control daemon                    3164 active
      Ilmi daemon                                        2132 active
      Remote operations daemon                           2964 active
      CoS daemon                                         3044 active
      Pic Services Logging daemon                        1944 active
      Internal Routing Service Daemon                    1392 active
      Network Access Service daemon                      1992 active
      Forwarding UDP daemon                              1876 active
      Routing socket proxy daemon                        1296 active
      Disk Monitoring daemon                             1180 active
      Inet daemon                                        1296 active
      Syslog daemon                                      1180 active
```

```
       Adaptive Services PIC daemon                     3220 active
       ECC parity errors logging Daemon                 1100 active
       Layer 2 Tunneling Protocol daemon                3372 active
       PPPoE daemon                                     1424 active
       Redundancy device daemon                         1820 active
       PPP daemon                                       2060 active
       Dynamic Flow Capture Daemon                     10740 active
 32780 Health Monitor: jroute daemon Memory utilization
       Routing protocol daemon                          8104 active
       Management daemon                               13360 active
       Management daemon                               19252 active
       Command line interface                           9912 active
       Periodic Packet Management daemon                1484 active
       Link Management daemon                           2016 active
       Pragmatic General Multicast daemon               1968 active
       Bidirectional Forwarding Detection daemon        1956 active
       SRC daemon                                       1772 active
       audit daemon                                     1772 active
       Event daemon                                     1808 active

 32781 Health Monitor: jcrypto daemon Memory utilization
       IPSec Key Management daemon                      5600 active
```

show snmp health-monitor alarms detail

user@host> **show snmp health-monitor alarms detail**

```
Alarm Index 32768:
  Variable name                       jnxHrStoragePercentUsed.1
  Variable OID                        1.3.6.1.4.1.2636.3.31.1.1.1.1.1
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: root file system
                                      utilization
  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 58
    Instance State: active
```

```
Alarm Index 32769:
  Variable name                        jnxHrStoragePercentUsed.2
  Variable OID                         1.3.6.1.4.1.2636.3.31.1.1.1.1.2
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                                Health Monitor: /config file system
                                       utilization
  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold                  80
  Falling threshold                 70
  Rising event index              32768
  Falling event index             32768
    Instance Value: 0
    Instance State: active

Alarm Index 32770:
  Variable name                        jnxOperatingCPU.9.1.0.0
  Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                               Health Monitor: RE 0 CPU utilization


  Creator                              Health Monitor
  State                                active
  Sample interval                  300 seconds
  Rising threshold                  80
  Falling threshold                 70
  Rising event index              32768
  Falling event index             32768
    Instance Value: 0
    Instance State: active

Alarm Index 32773:
  Variable name                        jnxOperatingBuffer.9.1.0.0
  Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0
  Sample type                          absolute value
  Startup alarm                        rising alarm
  Owner                               Health Monitor: RE 0 Memory utilization
```

```
  Creator                              Health Monitor
  State                                active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 35
    Instance State: active

Alarm Index 32775:
  Variable name                        sysApplElmtRunCPU.3
  Variable OID                         1.3.6.1.2.1.54.1.2.3.1.9.3
  Sample type                          delta value
  Startup alarm                        rising alarm
  Owner                                Health Monitor: jkernel daemon CPU
                                       utilization
  Creator                              Health Monitor
  State                                active
  Sample interval                 300 seconds
  Rising threshold              24000
  Falling threshold             21000
  Rising event index            32768
  Falling event index           32768
    Instance Name: sysApplElmtRunCPU.3.1.1
    Instance Description: Init daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.2.2786
    Instance Description: Chassis daemon
    Instance Value: 50
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.3.2938
    Instance Description: Firewall daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.4.2942
    Instance Description: Interface daemon
    Instance Value: 5
    Instance State: active
```

```
    Instance Name: sysApplElmtRunCPU.3.7.7332
    Instance Description: SNMP daemon
    Instance Value: 11
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.9.2914
    Instance Description: MIB2 daemon
    Instance Value: 42
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.12.2916
    Instance Description: Sonet APS daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.13.2917
    Instance Description: VRRP daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.14.2787
    Instance Description: Alarm daemon
    Instance Value: 3
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.15.2940
    Instance Description: PFE daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.16.2788
    Instance Description: CRAFT daemon
    Instance Value: 0
    Instance State: active

    Instance Name: sysApplElmtRunCPU.3.17.2918
    Instance Description: Traffic sampling control daemon
---(more 23%)---
```

show snmp inform-statistics

Syntax

```
show snmp inform-statistics
```

Release Information

Command introduced in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) inform requests.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show snmp inform-statistics on page 3084

Output Fields

Table 261 on page 2879 describes the output fields for the **show snmp inform-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 294: show snmp inform-statistics Output Fields

Field Name	Field Description
Target Name	Name of the device configured to receive and respond to SNMP informs.
Address	IP address of the target device.
Sent	Number of informs sent to the target device and acknowledged by the target device.
Pending	Number of informs held in memory pending a response from the target device.
Discarded	Number of informs discarded after the specified number of retransmissions to the target device were attempted.
Timeouts	Number of informs that did not receive an acknowledgement from the target device within the timeout specified.

Table 294: show snmp inform-statistics Output Fields *(continued)*

Field Name	Field Description
Probe Failures	Connection failures that occurred (for example, when the target server returned invalid content or you incorrectly configured the target address).

Sample Output

show snmp inform-statistics

```
user@host> show snmp inform-statistics
```

```
Inform Request Statistics:
 Target Name: TA1_v3_md5_none Address: 172.17.20.184
  Sent: 176, Pending: 0
  Discarded: 0, Timeouts: 0, Probe Failures: 0
 Target Name: TA2_v3_sha_none Address: 192.168.110.59
  Sent: 0, Pending: 4
  Discarded: 84, Timeouts: 0, Probe Failures: 258
 Target Name: TA5_v2_none Address: 172.17.20.184
  Sent: 0, Pending: 0
  Discarded: 2, Timeouts: 10, Probe Failures: 0
```

show snmp mib

Syntax

```
show snmp mib (get | get-next | walk) (ascii | decimal | hex) object-id
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
ascii and **decimal** options introduced in Junos OS Release 9.6.
ascii and **decimal** options introduced in Junos OS Release 9.6 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
hex option introduced in Junos OS Release 19.2R2.
Behavior in regard to sysName.0 MIB object changed in Junos OS Release 19.1R1.

Description

Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.

> **NOTE:** Starting in Junos OS Release 18.3R1, SNMP queue statistics reporting for static interface-sets configured over Aggregate Ethernet (AE) interfaces is supported.
>
> Starting in Junos OS Release 19.1R1, the sysName.0 MIB object displays the fully qualified domain name. That is, if the hostname and domain name are configured on the system, both will show up for the sysName.0 MIB object.

Starting in Junos OS Release 20.2R1, We've introduced the new SNMP MIBs **jnxJsSPUMonitoringSPUThreadsNumber**, **jnxJsSPUMonitoringSPUThreadIndex**, **jnxJsSPUMonitoringSPUThreadLastMinUsage**, **jnxJsSPUMonitoringSPUThreadLastHourUsage**, and **jnxJsSPUMonitoringSPUThreadLastDayUsage** to monitor the CPU usage information of an SPC3 card.

Options

get—Retrieve and display one or more SNMP object values.

get-next—Retrieve and display the next SNMP object values.

walk—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.

NOTE: As of Junos OS Release 18.4R1, the CLI configuration command **set snmp customization ether-stats-ifd-only** is introduced. When **ether-stats-ifd-only** is configured, the **show snmp mib walk etherstatsTable** command displays data only for physical interfaces (IFDs). See customization (SNMP).

ascii—Display the SNMP object's string indices as an ASCII-key representation.

decimal—Display the SNMP object values in the decimal (default) format. The **decimal** option is the default option for this command. Therefore, issuing the **show snmp mib (get | get-next | walk) decimal object-id** and the **show snmp mib (get | get-next | walk) object-id** commands display the same output.

hex—Display the SNMP object values in the hexadecimal format.

object-id—The object can be represented by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). When entering multiple objects, enclose the objects in quotation marks.

Required Privilege Level

snmp—To view this statement in the configuration.

List of Sample Output

show snmp mib get on page 3087
show snmp mib get (Routing Engine) on page 3087
show snmp mib get (Routing Engine, PTX10003) on page 3087
show snmp mib get (Multiple Objects) on page 3088
show snmp mib get (Layer 2 Policer) on page 3088
show snmp mib get-next on page 3088
show snmp mib get-next (Specify an OID) on page 3088
show snmp mib walk on page 3088
show snmp mib walk (QFX Series) on page 3089
show snmp mib walk (ASCII) on page 3089
show snmp mib walk (Multiple Indices) on page 3089
show snmp mib walk decimal on page 3089
show snmp mib walk decimal (Multiple Indices) on page 3089
show snmp mib walk hex on page 3090
show snmp mib walk (Queue Statistics) on page 3090
show snmp mib walk bgp (MX Series) on page 3091
show snmp mib walk mplsL3VpnMIB (MX Series) on page 3092
show snmp mib walk (PTX10003) on page 3092
show snmp mib walk ascii jnxWlanWAPStatusTable (SRX320, SRX340, SRX345, and SRX550M) on page 3093
show snmp mib walk jnxWlanWAPClientTable (SRX320, SRX340, SRX345, and SRX550M) on page 3094

show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber (SRX5400, SRX5600, and SRX5800) on page 3094
show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex (SRX5400, SRX5600, and SRX5800) on page 3094
show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 (SRX5400, SRX5600, and SRX5800) on page 3095
show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 (SRX5400, SRX5600, SRX5800) on page 3095
show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 (SRX5400, SRX5600, and SRX5800) on page 3095

Output Fields

Table 262 on page 2883 describes the output fields for the **show snmp mib** command. Output fields are listed in the approximate order in which they appear.

Table 295: show snmp mib Output Fields

Field Name	Field Description
name	Object name and numeric instance value.
object value	Object value. The Junos OS translates OIDs into the corresponding object names.

Sample Output

show snmp mib get

```
user@host> show snmp mib get sysObjectID.0
```

```
sysObjectID.0 = jnxProductNameM20
```

show snmp mib get (Routing Engine)

```
user@router> show snmp mib get jnxFruName.9.1.0.0
```

```
jnxFruName.9.1.0.0 = Routing Engine 0
```

show snmp mib get (Routing Engine, PTX10003)

```
user@router> show snmp mib get jnxFruName.9.1.0.0
```

```
jnxFruName.9.1.0.0 = Routing Engine slot 0
```

show snmp mib get (Multiple Objects)

user@host> **show snmp mib get "sysObjectID.0 sysUpTime.0"**

```
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

show snmp mib get (Layer 2 Policer)

user@host> **show snmp mib get ifInOctets.25970**

```
ifInOctets.25970 = 7545720
```

show snmp mib get-next

user@host> **show snmp mib get-next jnxMibs**

```
jnxBoxClass.0 = jnxProductLineM20.0
```

show snmp mib get-next (Specify an OID)

user@host> **show snmp mib get-next 1.3.6.1**

```
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper
 Networks, Inc.
```

show snmp mib walk

user@host> **show snmp mib walk system**

```
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004
Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
sysContact.0 = Your contact
sysName.0 = my router
```

```
sysLocation.0 = building 1
sysServices.0 = 4
```

show snmp mib walk (QFX Series)

`user@switch>` **show snmp mib walk system**

```
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 138980301
sysContact.0  = System Contact
sysName.0     = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

show snmp mib walk (ASCII)

`user@host>` **show snmp mib walk ascii jnxUtilData**

```
jnxUtilCounter32Value."fred" = 100
```

show snmp mib walk (Multiple Indices)

`user@host>` **show snmp mib walk ascii jnxFWCounterByteCount**

```
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```

show snmp mib walk decimal

`user@host>`**show snmp mib walk decimal jnxUtilData**

```
jnxUtilCounter32Value.102.114.101.100 = 100
```

show snmp mib walk decimal (Multiple Indices)

`user@host>` **show snmp mib walk ascii jnxFWCounterByteCount**

```
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```

show snmp mib walk hex

`user@host>` **show snmp mib walk hex jnxBgpM2PeerRemoteAddr**

```
jnxBgpM2PeerRemoteAddr.0.1.10.0.3.3.1.10.0.3.1 = 0a 00 03 01
jnxBgpM2PeerRemoteAddr.0.1.32.32.32.9.1.32.32.32.32 = 00 00 00 00
jnxBgpM2PeerRemoteAddr.0.1.62.40.96.38.1.62.40.96.19 = 3e 28 60 13
jnxBgpM2PeerRemoteAddr.0.1.62.40.96.38.1.62.40.96.39 = 3e 28 60 27
```

show snmp mib walk (Queue Statistics)

To get interface-set queue statistics from jnxCosQstatQedPkts MIB with using interface-set SNMP index, use the following command:

`show snmp mib walk jnxCosQstatQedPkts.`*`interface-set snmp index`*

For example, if the interface-set SNMP index is 67108866

`user@host>` **show snmp mib walk jnxCosQstatQedPkts.67108866**

```
jnxCosQstatQedPkts.67108866.0 = 10
jnxCosQstatQedPkts.67108866.1 = 0
jnxCosQstatQedPkts.67108866.2 = 0
jnxCosQstatQedPkts.67108866.3 = 0
jnxCosQstatQedPkts.67108866.4 = 0
jnxCosQstatQedPkts.67108866.5 = 0
jnxCosQstatQedPkts.67108866.6 = 0
jnxCosQstatQedPkts.67108866.7 = 0
```

To get interface-set queue statistics from jnxCosIfsetQstatQedPkts MIB with using interface-set SNMP index, use the following command:

`show snmp mib walk jnxCosIfsetQstatQedPkts.`*`interface-set snmp index`*

For example, if the interface-set snmp index is 67108866

`user@host>` **show snmp mib walk jnxCosIfsetQstatQedPkts.67108866**

```
jnxCosIfsetQstatQedPkts.67108866.0 = 10
jnxCosIfsetQstatQedPkts.67108866.1 = 0
jnxCosIfsetQstatQedPkts.67108866.2 = 0
jnxCosIfsetQstatQedPkts.67108866.3 = 0
jnxCosIfsetQstatQedPkts.67108866.4 = 0
jnxCosIfsetQstatQedPkts.67108866.5 = 0
jnxCosIfsetQstatQedPkts.67108866.6 = 0
jnxCosIfsetQstatQedPkts.67108866.7 = 0
```

To get Interface-set queue statistics from jnxCosIfsetQstatQedPkts MIB using interface-set member IFL SNMP index, use the following command:

`show snmp mib walk jnxCosIfsetQstatQedPkts.`*`interface-set member IFL SNMP index`*

For example, if the interface-set member IFL SNMP is 519

`user@host>` **show snmp mib walk jnxCosIfsetQstatQedPkts.519**

```
jnxCosIfsetQstatQedPkts.519.0 = 10
jnxCosIfsetQstatQedPkts.519.1 = 0
jnxCosIfsetQstatQedPkts.519.2 = 0
jnxCosIfsetQstatQedPkts.519.3 = 0
jnxCosIfsetQstatQedPkts.519.4 = 0
jnxCosIfsetQstatQedPkts.519.5 = 0
jnxCosIfsetQstatQedPkts.519.6 = 0
jnxCosIfsetQstatQedPkts.519.7 = 0
```

show snmp mib walk bgp (MX Series)

Use the **show snmp mib walk bgp** to see the BGP versions.

`user@host>` **show snmp mib walk bgp**

```
bgpVersion.0  = 10
bgpLocalAs.0  = 1
bgpPeerIdentifier.2.2.2.2 = 2.2.2.2
bgpPeerIdentifier.3.3.3.3 = 3.3.3.3

bgpPeerInUpdates.2.2.2.2 = 3
bgpPeerInUpdates.3.3.3.3 = 2
bgpPeerOutUpdates.2.2.2.2 = 1
bgpPeerOutUpdates.3.3.3.3 = 1
bgpPeerInTotalMessages.2.2.2.2 = 11
```

```
bgpPeerInTotalMessages.3.3.3.3 = 10
bgpPeerOutTotalMessages.2.2.2.2 = 8
bgpPeerOutTotalMessages.3.3.3.3 = 8
```

show snmp mib walk mplsL3VpnMIB (MX Series)

Use the **show snmp mib walk mplsL3VpnMIB** to see attributes of L3VPN based MPLS.

`user@host>` **show snmp mib walk mplsL3VpnMIB**

```
mplsL3VpnConfiguredVrfs.0 = 1
mplsL3VpnActiveVrfs.0 = 1
mplsL3VpnConnectedInterfaces.0 = 1
mplsL3VpnNotificationEnable.0 = 2
mplsL3VpnVrfConfMaxPossRts.0 = 0
mplsL3VpnVrfConfRteMxThrshTime.0 = 0
mplsL3VpnIllLblRcvThrsh.0 = 0
mplsL3VpnIfVpnClassification.3.114.101.100.548 = 2
mplsL3VpnIfVpnRouteDistProtocol.3.114.101.100.548 = 40 7f
mplsL3VpnIfConfStorageType.3.114.101.100.548 = 5
mplsL3VpnIfConfRowStatus.3.114.101.100.548 = 1
mplsL3VpnVrfVpnId.3.114.101.100
mplsL3VpnVrfDescription.3.114.101.100 = red
mplsL3VpnVrfRD.3.114.101.100 = 2:1
mplsL3VpnVrfCreationTime.3.114.101.100 = 9111800
mplsL3VpnVrfOperStatus.3.114.101.100 = 1
mplsL3VpnVrfActiveInterfaces.3.114.101.100 = 1
mplsL3VpnVrfAssociatedInterfaces.3.114.101.100 = 1
mplsL3VpnVrfConfMidRteThresh.3.114.101.100 = 0
mplsL3VpnVrfConfHighRteThresh.3.114.101.100 = 0
mplsL3VpnVrfConfMaxRoutes.3.114.101.100 = 0
mplsL3VpnVrfConfLastChanged.3.114.101.100 = 9111800
```

show snmp mib walk (PTX10003)

On PTX10003-80C and PTX10003-160C devices, the **show snmp mib walk jnxFilledDescr** output shows only the fan tray number. This output does not show the number of fan slots present in each tray.

`user@router>` **show snmp mib walk jnxFilledDescr**

```
jnxFilledDescr.1.0.0.0 = Chassis
jnxFilledDescr.4.2.0.0 = Fan Tray 1
jnxFilledDescr.4.3.0.0 = Fan Tray 2
jnxFilledDescr.4.4.0.0 = Fan Tray 3
[...Output truncated...]
```

show snmp mib walk ascii jnxWlanWAPStatusTable (SRX320, SRX340, SRX345, and SRX550M)

Use the **show snmp mib walk ascii jnxWlanWAPStatusTable** command to monitor the Wi-Fi Mini-Physical Interface Module (Mini-PIM) status.

`user@host>` **show snmp mib walk ascii jnxWlanWAPStatusTable**

```
jnxWAPStatusIfdIndex.161 = 161
jnxWAPStatusIfdIndex.162 = 162
jnxWAPStatusAccessPoint.161 = bj345b_wl3_wap
jnxWAPStatusAccessPoint.162 = bj345b_wap
jnxWAPStatusType.161 = Internal
jnxWAPStatusType.162 = Internal
jnxWAPStatusLocation.161 = Default Location
jnxWAPStatusLocation.162 = Default Location
jnxWAPStatusSerialNumber.161
jnxWAPStatusSerialNumber.162
jnxWAPStatusFirmwareVersion.161 = v1.1.0
jnxWAPStatusFirmwareVersion.162 = v1.1.0
jnxWAPStatusAlternateVersion.161 = v1.1.0
jnxWAPStatusAlternateVersion.162 = v1.1.0
jnxWAPStatusCountry.161 = US
jnxWAPStatusCountry.162 = US
jnxWAPStatusAccessInterface.161 = wl-3/0/0
jnxWAPStatusAccessInterface.162 = wl-4/0/0
jnxWAPStatusSystemTime.161 = Fri Jun 21 05:05:42 UTC 2019
jnxWAPStatusSystemTime.162 = Fri Jun 21 05:38:46 UTC 2019
jnxWAPStatusPacketCapture.161 = Off
jnxWAPStatusPacketCapture.162 = Off
jnxWAPStatusEthernetPortMAC.161 = 56:48:0d:5e:8f:c5
jnxWAPStatusEthernetPortMAC.162 = 8a:b7:0a:7e:ad:8a
jnxWAPStatusEthernetIPv4.161
jnxWAPStatusEthernetIPv4.162
jnxWAPStatusRadio1Status.161 = On
jnxWAPStatusRadio1Status.162 = On
[...Output truncated...]
```

show snmp mib walk jnxWlanWAPClientTable (SRX320, SRX340, SRX345, and SRX550M)

Use the **show snmp mib walk jnxWlanWAPClientTable** command to monitor the Wi-Fi Mini-PIM client information.

`user@host>` **show snmp mib walk jnxWlanWAPClientTable**

```
jnxWAPClientIfdIndex.161.1 = 161
jnxWAPClientIfdIndex.162.1 = 162
jnxWAPClientIfdIndex.162.2 = 162
jnxWAPClientIndex.161.1 = 1
jnxWAPClientIndex.162.1 = 1
jnxWAPClientIndex.162.2 = 2
jnxWAPClientRadioID.161.1 = 1
jnxWAPClientRadioID.162.1 = 1
jnxWAPClientRadioID.162.2 = 1
jnxWAPClientSSID.161.1 = bj345b_wl3_5g
jnxWAPClientSSID.162.1 = bj345b_5g
jnxWAPClientSSID.162.2 = bj345b_5g
jnxWAPClientMAC.161.1 = e8:4e:06:64:38:89
jnxWAPClientMAC.162.1 = e8:4e:06:64:38:a3
jnxWAPClientMAC.162.2 = e8:4e:06:63:9d:f6
jnxWAPClientAuth.161.1 = NO
[...Output truncated...]
```

show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber** command to list the indices of flow threads in an SPU.

`user@host>` **show snmp mib walk jnxJsSPUMonitoringSPUThreadsNumber**

```
jnxJsSPUMonitoringSPUThreadsNumber.4 = 26
jnxJsSPUMonitoringSPUThreadsNumber.5 = 26
jnxJsSPUMonitoringSPUThreadsNumber.16 = 0
jnxJsSPUMonitoringSPUThreadsNumber.17 = 0
jnxJsSPUMonitoringSPUThreadsNumber.18 = 0
jnxJsSPUMonitoringSPUThreadsNumber.19 = 0
```

show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex** command to list the indices of flow threads in an SPU.

user@host> **show snmp mib walk jnxJsSPUMonitoringSPUThreadIndex**

```
jnxJsSPUMonitoringSPUThreadIndex.4.0 = 0
jnxJsSPUMonitoringSPUThreadIndex.4.1 = 1
jnxJsSPUMonitoringSPUThreadIndex.4.2 = 2
jnxJsSPUMonitoringSPUThreadIndex.4.3 = 3

... ...

jnxJsSPUMonitoringSPUThreadIndex.5.22 = 22
jnxJsSPUMonitoringSPUThreadIndex.5.23 = 23
jnxJsSPUMonitoringSPUThreadIndex.5.24 = 24
jnxJsSPUMonitoringSPUThreadIndex.5.25 = 25
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8** command to monitor the average CPU usage for the last minute on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastMinUsage.5.8 = 0
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 (SRX5400, SRX5600, SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8** command to monitor the average CPU usage for the last hour on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastHourUsage.5.8 = 0
```

show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 (SRX5400, SRX5600, and SRX5800)

Use the **show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8** command to monitor the average CPU usage for the last 24 hours on the specified thread.

user@host> **show snmp mib get jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8**

```
jnxJsSPUMonitoringSPUThreadLastDayUsage.5.8 = 0
```

show snmp rmon

Syntax

```
show snmp rmon
<alarms <brief | detail> | events <brief | detail> | logs>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms, events, and logs.

Options

none—Display information about all RMON alarms and events.

alarms—(Optional) Display information about RMON alarms.

brief | detail—(Optional) Display brief or detailed information about RMON alarms or events.

events—(Optional) Display information about RMON events.

logs—(Optional) Display information about RMON monitoring logs.

Required Privilege Level

view

RELATED DOCUMENTATION

- RMON MIB Event, Alarm, Log, and History Control Tables | **781**
- Monitoring RMON MIB Tables | **642**
- Configuring RMON Alarms and Events | **652**
- Understanding RMON | **774**
- clear snmp statistics | **2860**
- clear snmp history | **2969**
- show snmp rmon history | **2899**

List of Sample Output

show snmp rmon on page 3100
show snmp rmon (QFX Series) on page 3100
show snmp rmon alarms detail on page 3101
show snmp rmon events detail on page 3101
show snmp rmon logs (QFX Series) on page 3102

Output Fields

Table 263 on page 2894 describes the output fields for the **show snmp rmon** command. Output fields are listed in the approximate order in which they appear.

Table 296: show snmp rmon Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
State	State of the alarm or event entry: Alarms: • **active**—Entry is fully configured and activated. • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit. • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit. • **under creation**—Entry is being configured and is not yet activated. • **startup**—Alarm is waiting for the first sample of the monitored variable. • **object not available**—Monitored variable of that type is not available to the SNMP agent. • **instance not available**—Monitored variable's instance is not available to the SNMP agent. • **object type invalid**—Monitored variable is not a numeric value. • **object processing errored**—An error occurred when the monitored variable was processed. • **unknown**—State is not one of the above. Events: • **active**—Entry has been fully configured and activated. • **under creation**—Entry is being configured and is not yet activated. • **unknown**—State is not one of the above.	All levels
Variable name	Name of the SNMP object instance being monitored.	All levels
Event Index	Event identifier.	All levels

Table 296: show snmp rmon Output Fields *(continued)*

Field Name	Field Description	Level of Output
Type	Type of notification made when an event is triggered. It can be one of the following: • **log**—A system log message is generated and an entry is made to the log table. • **snmptrap**—An SNMP trap is sent to the configured destination. • **log and trap**—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination. • **none**—Neither log nor trap will be sent.	**detail**
Last Event	Date and time of the last event. It has the format *yyyy-mm-dd hh:mm:ss timezone*.	**brief**
Community	Trap group used for sending the SNMP trap.	**detail**
Variable OID	Object ID to which the variable name is resolved. The format is **x.x.x.x**.	**detail**
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**.	**detail**

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.
	• Alarm is *not* sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.
	  ◦ Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	**detail**
Creator	Mechanism by which the entry was configured (**CLI** or **SNMP**).	**detail**

Table 296: show snmp rmon Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sample interval	Time period between samples (in seconds).	**detail**
Rising threshold	Upper limit threshold value configured by the user.	**detail**
Falling threshold	Lower limit threshold value configured by the user.	**detail**
Rising event index	Event triggered when the rising threshold is crossed.	**detail**
Falling event index	Event triggered when the falling threshold is crossed.	**detail**
Current value	Current value of the monitored variable in the most recent sample interval.	**detail**

Sample Output

show snmp rmon

```
user@host> show snmp rmon
```

```
Alarm
Index  State                       Variable name
    1  falling threshold crossed   ifInOctets.1

Event
Index  Type                        Last Event
    1  log and trap                2002-01-30 01:13:01 PST
```

show snmp rmon (QFX Series)

```
user@host> show snmp rmon
```

```
Alarm
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                          5 falling threshold
```

```
Event
Index  Type                          Last Event
    1  log and trap                  2009-07-10 11:34:17 PDT
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```

show snmp rmon alarms detail

user@host> **show snmp rmon alarms detail**

```
Alarm Index 1:
  Variable name                       ifInOctets.1
  Variable OID                        1.3.6.1.2.1.2.2.1.10.1
  Sample type                         delta value
  Startup alarm                       rising or falling alarm
  Owner                               monitor
  Creator                             CLI
  State                               falling threshold crossed
  Sample interval                  60 seconds
  Rising threshold             100000
  Falling threshold             80000
  Rising event index                1
  Falling event index               1
  Current value                     0
```

show snmp rmon events detail

user@host> **show snmp rmon events detail**

```
Event Index 1:
  Description                         rmon event
  Type                                log and trap
  Community                           rmon-trap-group
  Last event                          2009-07-10 11:34:17 PDT
  Creator                             CLI
  State                               active
```

show snmp rmon logs (QFX Series)

user@host> **show snmp rmon logs**

```
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```

show snmp statistics

Syntax

```
show snmp statistics
<subagents>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Option **subagents** introduced in Junos OS Release 14.2.

Description

Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

Options

subagents—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

Required Privilege Level

view

RELATED DOCUMENTATION

clear snmp statistics | **2860**

List of Sample Output

show snmp statistics on page 3108
show snmp statistics subagents on page 3108

Output Fields

Table 265 on page 2905 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 297: show snmp statistics Output Fields

Field Name	Field Description
Input	Information about received packets: • **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service. • **Bad versions**—**(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. • **Bad community names**—**(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. • **Bad community uses**—**(snmpInBadCommunityUses)** Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. • **ASN parse errors**—**(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. • **Too bigs**—**(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**. • **No such names**—**(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values**—**(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**. • **Read onlys**—**(snmpInReadOnlys)** Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of **readOnly**. Only incorrect implementations of SNMP generate this error.

Table 297: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Input (continued)	• **General errors**—**(snmpInGenErrs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **genErr**. • **Total requests varbinds**—**(snmpInTotalReqVars)** Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP **GetRequest** and **GetNext** PDUs. • **Total set varbinds**—**(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs. • **Get requests**—**(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get nexts**—**(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity. • **Set requests**—**(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get responses**—**(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity. • **Traps**—**(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity. • **Silent drops**—**(snmpSilentDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • **Proxy drops**—**(snmpProxyDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration. • **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit.

Table 297: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
V3 Input	Information about SNMP version 3 packets: • **Unknown security models—(snmpUnknownSecurityModels)** Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • **Invalid messages—(snmpInvalidMsgs)** Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • **Unknown pdu handlers—(snmpUnknownPDUHandlers)** Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine. • **Unsupported security levels—(usmStatsUnsupportedSecLevels)** Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • **Not in time windows—(usmStatsNotInTimeWindows)** Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • **Unknown user names—(usmStatsUnknownUserNames)** Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • **Unknown engine ids—(usmStatsUnknownEngineIDs)** Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 297: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Output	Information about transmitted packets: • **Packets**—**(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service. • **Too bigs**—**(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**. • **No such names**—**(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values**—**(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**. • **General errors**—**(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**. • **Get requests**—**(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity. • **Get nexts**—**(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity. • **Set requests**—**(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity. • **Get responses**—**(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity. • **Traps**—**(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity.

Table 266 on page 2908 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 298: show snmp statistics subagents Output Fields

Field Name	Field Description
Subagent	Location of the SNMP subagent.
Request PDUs	Number of PDUs requested by the SNMP manager.
Response PDUs	Number of response PDUs sent by the SNMP subagent.
Request Variables	Number of variable bindings on the PDUs requested by the SNMP manager.
Response Variables	Number of variable bindings on the PDUs sent by the SNMP subagent.
Average Response Time	Average time taken by the SNMP subagent to send statistics response.

Table 298: show snmp statistics subagents Output Fields *(continued)*

Field Name	Field Description
Maximum Response Time	Maximum time taken by the SNMP subagent to send the statistics response.

Sample Output

show snmp statistics

```
user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12,
    Bad community uses: 0, ASN parse errors: 96,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 227084, Total set varbinds: 67,
    Get requests: 44942, Get nexts: 190371, Set requests: 10712,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0,
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 1
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
  Output:
    Packets: 246093, Too bigs: 0, No such names: 31561,
    Bad values: 0, General errors: 2,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 246025, Traps: 0
```

show snmp statistics subagents

```
user@host> show snmp statistics subagents

  Subagent: /var/run/cosd-20
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
```

```
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/pfed-30
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rmopd-15
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/chassisd-30
  Request PDUs: 33116, Response PDUs: 33116,
  Request Variables: 33116, Response Variables: 33116,
  Average Response Time(ms): 1.83,
  Maximum Response Time(ms): 203.48

Subagent: /var/run/pkid-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,
  Request Variables: 74211, Response Variables: 74211,
  Average Response Time(ms): 2.30,
  Maximum Response Time(ms): 51.04
```

```
Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
```

show snmp stats-response-statistics

Syntax

```
show snmp stats-response-statistics
```

Release Information

Command introduced in Junos OS Release 14.2.

Description

Display statistics of SNMP statistics responses sent from the Packet Forwarding Engine during the MIB II process (mib2d).

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show snmp stats-response-statistics on page 3112

Output Fields

Table 299 on page 3111 describes the output fields for the **show snmp stats-response-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 299: show snmp stats-response-statistics Output Fields

Field Name	Field Description
Average response time statistics	Display the average response time in milliseconds per protocol data unit (PDU) by snmpd. It includes the following information: • **Stats Type**—Type of SNMP statistics. • **Stats Responses**—Number of SNMP statistics responses received from the Packet Forwarding Engine. • **Average Response Time**—Average time taken to receive the statistics response from the Packet Forwarding Engine in milliseconds.
Bucket statistics	Information about SNMP statistics responses: • **Bucket Type**—Category of time intervals in which SNMP statistics responses are received from the Packet Forwarding Engine. • **Stats Responses**—Number of SNMP statistics responses received from the Packet Forwarding Engine.

Table 299: show snmp stats-response-statistics Output Fields *(continued)*

Field Name	Field Description
Bad responses	Information about top 20 bad responses from a subagent: • **Response**—Time taken to receive the SNMP statistics response from the Packet Forwarding Engine in milliseconds. • **Request Time**—Date and time of SNMP request. • **Key**—Display the attribute of SNMP **Stats Type**. For example, in the case of SNMP statistics responses for interfaces, the Key value is SNMP ifIndex, and for firewalls, the Key value is the filter name.

Sample Output

show snmp stats-response-statistics

```
user@host> show snmp stats-response-statistics
```

```
Average response time statistics:
Stats                Stats                   Average
Type                 Responses               Response
                                             Time (ms)
ifd(non ae)          34182                   175.48
ifd(ae)              0                       0.00
ifl(non ae)          5472                    5.40
ifl(ae)              0                       0.00
firewall             15                      1141.73

Bucket statistics:
Bucket               Stats
Type(ms)             Responses
0 - 10               39078
11 - 50              588
51 - 100             0
101 - 200            0
201 - 500            1
501 - 1000           2
1001 - 2000          0
2001 - 5000          0
More than 5001       0

Bad responses:
```

```
Response        Request                Stats          Key
                Time                   Type
(ms)            (UTC)
927.80          2014-03-26 05:44:16    firewall       __default_arp_policer__
908.68          2014-03-26 05:44:16    firewall       __default_bpdu_filter__
421.00          2014-03-26 05:46:25    ifd(non ae)    504
49.76           2014-04-13 04:15:18    ifd(non ae)    503
49.62           2014-04-13 04:30:18    ifd(non ae)    504
48.52           2014-04-05 10:06:55    ifd(non ae)    504
47.61           2014-04-11 04:06:27    ifd(non ae)    505
47.38           2014-04-13 03:30:18    ifd(non ae)    501
47.22           2014-03-27 20:08:07    ifd(non ae)    502
46.26           2014-03-31 13:08:58    ifd(non ae)    506
46.00           2014-04-13 04:00:18    ifd(non ae)    503
45.95           2014-04-05 17:15:17    ifd(non ae)    503
45.75           2014-04-15 13:06:10    ifd(non ae)    507
45.60           2014-04-01 03:07:28    ifd(non ae)    517
45.56           2014-04-08 13:09:15    ifd(non ae)    502
45.23           2014-04-13 03:15:18    ifd(non ae)    501
45.15           2014-04-05 16:45:17    ifd(non ae)    501
44.74           2014-04-08 22:08:47    ifd(non ae)    505
44.10           2014-04-05 16:30:17    ifd(non ae)    501
44.00           2014-04-08 09:09:23    ifd(non ae)    524
```

show snmp v3

Syntax

```
show snmp v3
<access <brief | detail> | community | general | groups | notify <filter> | target <address | parameters> | users>
```

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 Simple Network Management Protocol version 3 (SNMPv3) operating configuration.

Options

none—Display all of the SNMPv3 operating configuration.

access—(Optional) Display SNMPv3 access information.

brief | detail—(Optional) Display brief or detailed information about SNMPv3 access information.

community—(Optional) Display SNMPv3 community information.

general—(Optional) Display SNMPv3 general information.

groups—(Optional) Display SNMPv3 security-to-group information.

notify <filter>—(Optional) Display SNMPv3 notify and, optionally, notify filter information.

target <address | parameters>—(Optional) Display SNMPv3 target and, optionally, either target address or target parameter information.

users—(Optional) Display SNMPv3 user information.

Additional Information

To edit the default display of the **show snmp v3** command, specify options in the **show** statement at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

view

List of Sample Output

show snmp v3 on page 3116

Output Fields

Table 267 on page 2913 describes the output fields for the **show snmp v3** command. Output fields are listed in the approximate order in which they appear.

Table 300: show snmp v3 Output Fields

Field Name	Field Description
Access control	Information about access control: • **Group**—Group name for which the configured access privileges apply. The group, together with the context prefix and the security model and security level, forms the index for this table. • **Context prefix**—SNMPv3 context for which the configured access privileges apply. • **Security model/level**—Security model and security level for which the configuration access privileges apply. • **Read view**—Identifies the MIB view applied to SNMPv3 read operations. • **Write view**—Identifies the MIB view applied to SNMPv3 write operations. • **Notify view**—Identifies the MIB view applied to outbound SNMP notifications.
Engine	Information about local engine configuration: • **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • **Max msg size**—Maximum message size the sender can accommodate.
Engine ID	Information about engine ID: • **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • **Max msg size**—Maximum message size the sender can accommodate. • **Engine ID**—SNMPv3 engine ID associated with each user. • **User**—SNMPv3 user. • **Auth/Priv**—Authentication and encryption algorithm available for use by each user. • **Storage**—Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status. • **Status**—Status of the conceptual row. Only rows with an active status are used by the SNMPv3 engine.
Group name	Name of the group to which this entry belongs.

Table 300: show snmp v3 Output Fields *(continued)*

Field Name	Field Description
Security model	Identifies the security model context for the security name.
Security name	Used with the security model; identifies a specific security name instance. Each security model/security name combination can be assigned to a specific group.
Storage type	Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.
Status	Status of the conceptual row. Only rows with active status are used by the SNMPv3 engine.

Sample Output

show snmp v3

```
user@host> show snmp v3
```

```
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots:          38
Engine time:        64583 seconds
Max msg size:        2048 bytes

Engine ID: local
    User                            Auth/Priv   Storage      Status
    user1                            md5/des    nonvolatile  active
    user2                            sha/none   nonvolatile  active
    user3                           none/none   nonvolatile  active

Engine ID: 81 00 0a 4c 04 64 64 64 64
    User                            Auth/Priv   Storage      Status
    UNEW                             md5/none   nonvolatile  active
Group name           Security  Security             Storage      Status
                     model     name                 type
g1                   usm       user1                nonvolatile  active
g2                   usm       user2                nonvolatile  active
g3                   usm       user3                nonvolatile  active

Access control:
Group                Context Security      Read       Write     Notify
                     prefix  model/level   view       view      view
```

```
g1                              usm/privacy  v1          v1
g2                              usm/authent  v1          v1
g3                              usm/none     v1          v1
```

show system alarms

Syntax

```
show system alarms
```

Release Information

Command introduced in Junos OS Release 11.1 for SRX Series devices.

Description

Display active system alarms.

Options

This command has no options.

Additional Information

System alarms are preset. You cannot modify them, although you can configure them to appear automatically in the J-Web user interface or CLI. They include a **configuration** alarm that appears when no rescue configuration alarm is set and a **license** alarm that appears when a software feature is configured but no valid license is configured for the feature.

Required Privilege Level

admin

List of Sample Output

show system alarms on page 3118

Sample Output

show system alarms

```
user@host> show system alarms
```

```
5 alarms currently active
Alarm time               Class  Description
2012-05-29 16:47:18 UTC  Major  /var partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /var partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Major  /root partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /root partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Minor  Rescue configuration is not set
```

show system alarms

Syntax

```
show system alarms
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display active system alarms. System alarms are software or operating system software related alarms. System alarms indicate a missing rescue configuration or software license, where valid. System alarms are preset. You cannot modify them, although you can configure them to appear automatically in the J-Web user interface or CLI. They include a *configuration* alarm that appears when no rescue configuration alarm is set and a *license* alarm that appears when a software feature is configured and no valid license is configured for the feature. You can also determine when a license will expire from syslog messages that appear starting from four weeks before expiry of the license. On EX6200 switches, an alarm can be triggered by an internal link error.

Chassis alarms indicate a failure on the device or one of its components. For example, chassis alarms include an alarm for fan tray failure on a device, or if an FPC on a device is unreachable. Chassis alarms are preset and cannot be modified.

Options

This command has no options.

Additional Information

The the logic for multiple feature licenses is based on the highest validity among the licenses. Also, for capacity non-cumulative, exclusive type licenses (such as for scale), the logic is based on the highest validity of the license.

> **NOTE:** As of Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The newer behavior has the about-to-expire logic based on the first expiring license.

In Junos OS release 11.1 and later, alarms for fans also show the slot number of the malfunctioning fans in the CLI output.

Starting with Junos OS Release 13.2, you can view degraded fabric alarms on a routing matrix based on TX Matrix Plus router with 3D SIBs. The alarm indicates that the source FPC is running with a degraded fabric condition. This alarm is an early warning of a possible fabric black-hole condition. When the degraded fabric alarm is raised on the source FPC, you can take remedial action to avoid a fabric black-hole condition. The degraded fabric alarm is raised on the source FPC if both the following conditions are met:

- The active Packet Forwarding Engine destinations are reachable on one or no active switching planes.
- At least one of the inactive switching planes has a fault that causes the destination Packet Forwarding Engine to become unreachable.

> **NOTE:** On Junos OS Evolved, the **show system alarms** command does not display the error number. Instead, you can use the **show chassis fpc errors detail** and the **show system errors** commands to list the errors that contribute to a failure.

Required Privilege Level
view

RELATED DOCUMENTATION

> Alarm Overview | **888**
>
> *show chassis alarms*

List of Sample Output
show system alarms on page 3121
show system alarms (Fan Tray) on page 3121
show system alarms (QFX Series and OCX Series) on page 3121
show system alarms (EX6200) on page 3122
show system alarms (TX Matrix Plus router with 3D SIBs) on page 3122
show system alarms (Junos OS Evolved) on page 3122

Output Fields

Table 301 on page 3121 lists the output fields for the **show system alarms** command. Output fields are listed in the approximate order in which they appear.

Table 301: show system alarms Output Fields

Field Name	Field Description
Alarm time	Date and time the alarm was first recorded.
Class	Severity class for this alarm: **Minor** or **Major**.
Description	Information about the alarm.

Sample Output

show system alarms

`user@host>` **show system alarms**

```
2 alarms currently active
Alarm time                  Class     Description
2005-02-24 17:29:34 UTC      Minor    IPsec VPN tunneling usage requires a license
2005-02-24 17:29:34 UTC       Minor     Rescue configuration is not sent
```

show system alarms (Fan Tray)

`user@host>` **show system alarms**

```
4 alarms currently active
Alarm time               Class  Description
2010-11-11 20:27:38 UTC  Major  Side Fan Tray 7 Failure
2010-11-11 20:27:13 UTC  Minor  Side Fan Tray 7 Overspeed
2010-11-11 20:27:13 UTC  Major  Side Fan Tray 5 Failure
2010-11-11 20:27:13 UTC  Major  Side Fan Tray 0 Failure
```

show system alarms (QFX Series and OCX Series)

`user@switch>` **show system alarms**

```
2 alarms currently active
Alarm time Class Description
2005-02-24 17:29:34 UTC Minor Rescue configuration is not sent
```

show system alarms (EX6200)

```
user@switch> show system alarms
```

```
2 alarms currently active
Alarm time               Class  Description
2013-04-05 16:51:41 PDT  Major  FPC 8 internal link errors detected
2013-04-04 18:05:35 PDT  Minor  Rescue configuration is not set
```

show system alarms (TX Matrix Plus router with 3D SIBs)

```
user@router> show system alarms
```

```
sfc0-re0:
--------------------------------------------------------------------------
2 alarms currently active
Alarm time               Class  Description
2013-05-08 18:13:58 UTC  Major  LCC 0 Major Errors
2013-05-08 17:48:46 UTC  Major  LCC 7 Major Errors

lcc0-re1:
--------------------------------------------------------------------------
1 alarm currently active
Alarm time               Class  Description
2013-05-08 18:19:24 UTC  Major  FPC 1 degraded fabric condition detected

lcc7-re0:
--------------------------------------------------------------------------
1 alarm currently active
Alarm time               Class  Description
2013-05-08 18:19:24 UTC  Major  FPC 7 degraded fabric condition detected
```

show system alarms (Junos OS Evolved)

```
user@router> show system alarms
```

```
10 alarms currently active
Alarm time               Class  Description
2019-02-01 02:20:09 PST  Major  PCI Corrected error on dev 0000:00:01.0
```

Starting in Junos OS Evolved Release 19.1R1, the alarm string for PCI Corrected error is shown as **PCI Corrected error on dev 0000:00:01.0**. Also, a PCI uncorrectable error does not cause a reboot, but only raises an alarm.

show system khms-stats

Syntax

```
show system khms-stats
<detail>
```

Release Information

Command introduced in Junos OS 19.3R1.

Description

Display information about interface states and statistics for next hop and memory usage.

Options

detail—Display information about kernel health parameters, such as graceful Routing Engine switchover (GRES) and in-service software upgrade (ISSU).

Required Privilege Level

View

List of Sample Output

show system khms-stats on page 3124
show system khms-stats detail on page 3126

Sample Output

show system khms-stats

`user@host>` **show system khms-stats**

```
Memory usage by ifstates, routes, nexthops, gencfg blobs
================================================================================
Memory type  Total no. of states     Memory used  Percentage of Dead states
     Ifstate                885           525KB             0%
      Routes                150            25KB             0%
     Nexthop                163            39KB             0%

Number of delayed unrefs of RT and NH: 0 (Max allowed 40000)

Number of delayed weight unrefs of RT and NH: 0 (Max allowed 400000)

Mbufs/Cluster Usage
```

```
=====================================================
852/1938/2790 mbufs in use (current/cache/total)
772/1198/1970/250436 mbuf clusters in use (current/cache/total/max)
769/1002 mbuf+clusters out of packet secondary zone in use (current/cache)
0/19/19/125218 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0/37101 9k jumbo clusters in use (current/cache/total/max)
0/0/0/20869 16k jumbo clusters in use (current/cache/total/max)
1757K/2956K/4713K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile

Memory Pages stats
=====================================================
Free pages threshold: 19226
Number of Free pages: 118312
Number of pages on buffer cache: 0

IFL Index space usage
=====================================================
MAX Number of Logical Interfaces(IFL's): 262144
Number of Logical Interfaces in use: 23
Number of Invalidated Logical Interfaces: 0


NH Index Space Allocation
=====================================================
    Index_Space_type             Used        Available
            Reserved               64             1280
             Private               39              665
             Regular               60          1046466
            Extended                0         15728638

Maximum possible number of private nexthops: 704
Percentage of private nexthop index space reserved for IRI:(internal routing) 30
Number of nexthop indices reserved for IRI:(internal routing) 212

Printing gencfg blobs statistics by major type

                                Type   Num Blobs   Data size
                     Proxy gencfg           33           0
                L2 forwarding blob            1         128
```

```
                          COS BLOB          41       36996
                   Feature License           1           2
                          Firewall          21        4044
                           CH Info           1           0
               Libpeer PeerInfo blob           2        4392
                         Resync blob           4          44
                         MACSEC blob           1           8
                         Agentd blob           4        5888
                       RPD EVPN blob           1          52
                           LFM Blob           1           8
                              Total         111       51562
```

show system khms-stats detail

user@host> **show system khms-stats detail**

```
Memory usage by ifstates, routes, nexthops, gencfg blobs
================================================================================
Memory type  Total no. of states     Memory used  Percentage of Dead states
     Ifstate                885           525KB             0%
      Routes                150            25KB             0%
     Nexthop                163            39KB             0%

Number of delayed unrefs of RT and NH: 0 (Max allowed 40000)

Number of delayed weight unrefs of RT and NH: 0 (Max allowed 400000)

Mbufs/Cluster Usage
=======================================================
852/1938/2790 mbufs in use (current/cache/total)
772/1198/1970/250436 mbuf clusters in use (current/cache/total/max)
769/1002 mbuf+clusters out of packet secondary zone in use (current/cache)
0/19/19/125218 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0/37101 9k jumbo clusters in use (current/cache/total/max)
0/0/0/20869 16k jumbo clusters in use (current/cache/total/max)
1757K/2956K/4713K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile

Memory Pages stats
=======================================================
```

```
Free pages threshold: 19226
Number of Free pages: 118117
Number of pages on buffer cache: 0

IFL Index space usage
=====================================================
MAX Number of Logical Interfaces(IFL's): 262144
Number of Logical Interfaces in use: 23
Number of Invalidated Logical Interfaces: 0


Kernel Health Parameters:
------------------------
  Record Time                       : 1568295214   : Thu Sep 12 19:03:34 2019

  Security:
    Veriexec                        : 3            :
VERIEXEC_STATE_ACTIVE_AND_LOADED

   Ifstate:
    Alive Ifstate count             : 883
    Dead Ifstate count              : 0
    Delayed Unrefs count            : 0
    Delayed Unrefs max              : 40000
    Stuck Ifstate clients           : 0
    Alive Ifstate clients           : 40
    Dead Ifstate clients            : 0
    Ifstate client limit reached    : 0

  GRES:
    GRES time (mastership acquired) : 0            : NA
    Protocol Slave Connect time     : 0            : NA
    GRES Configured state           : 0            : NOT_CONFIGURED
    Master Kernel GRES Ready        : 0            : GRES_NOT_READY
    Slave Kernel GRES Ready         : 0            : GRES_NOT_READY
    GRES Error state                : 0            : KSYNCD_NO_ERROR
    GRES Other RE Present           : 1            : OTHER_RE_PRESENT
    GRES Other RE Alive             : 1            : OTHER_RE_ALIVE
    GRES Is Protocol Master         : 1            : PROTOCOL_MASTER

  ISSU:
    ISSU Failure stage              : 0            : ISSU_STATE_IDLE
    Current ISSU stage              : 0            : ISSU_STATE_IDLE
```

```
Peer Infra:
  PFEMAN connection drops         : 0
  Spurious PPT wakeups            : 0

TNP:
  tnp hello drop count            : 0
  tnp fragment drop count         : 1

VPLS:
  unicast token count             : 0
  unicast token max               : 131072
  flood token count               : 1
  flood token max                 : 327680

TUNNEL:
  rpf tunnelid count              : 0
  rpf tunnelid MAX                : 1048575
  non-rpf tunnelid count          : 0
  non-rpf tunnelid MAX            : 15728640
  looped count                    : 0

MULTICAST:
  iif mismatch error count        : 0
  resolve request error count     : 0

RTSOCK:
  RTSOCK Total Veto               : 0
  RTSOCK Total Error              : 57

Aggregated Devices:
  PS LT Unstacking error count    : 0
  PS IFL l2circuit down count     : 0
  RLT LP Backup link down count   : 0
  AE Unstacking error count       : 0
  AE LP Backup link down count    : 0

TCPIP:
  Maximum Public nexthops         : 1046526
  Used  Public nexthops           : 68
  Maximum Private nexthops        : 704
  Used Private nexthops           : 35
  RTB Clone Route cnt             : 6
  RTB Clone Route Max             : 1000000
  ARP cache iri max               : 200
```

```
    ARP cache mgmt max              : 14960
    ARP cache public max            : 59840
    ARP cache iri cnt               : 4
    ARP cache mgmt cnt              : 2
    ARP cache public cnt            : 0
    ARP cache iri drop cnt          : 0
    ARP cache mgmt drop cnt         : 0
    ARP cache public drop cnt       : 0
    NDP cache iri max               : 200
    NDP cache mgmt max              : 14960
    NDP cache public max            : 59840
    NDP cache iri cnt               : 3
    NDP cache mgmt cnt              : 0
    NDP cache public cnt            : 0
    NDP cache iri drop cnt          : 0
    NDP cache mgmt drop cnt         : 0
    NDP cache public drop cnt       : 0
    Netisr queue ether wm cnt       : 0
    Netisr queue ether drop cnt     : 0
    Netisr queue ether pkt handled  : 524311
    Netisr queue ether pkt queued   : 524311
    Netisr queue ip wm cnt          : 0
    Netisr queue ip drop cnt        : 0
    Netisr queue ip pkt handled     : 451581
    Netisr queue ip pkt queued      : 451581
    Netisr queue ip6 wm cnt         : 0
    Netisr queue ip6 drop cnt       : 0
    Netisr queue ip6 pkt handled    : 2
    Netisr queue ip6 pkt queued     : 2
    Netisr queue arp wm cnt         : 0
    Netisr queue arp drop cnt       : 0
    Netisr queue arp pkt handled    : 50420
    Netisr queue arp pkt queued     : 50420
    TCP DDOS attack count           : 0
    TCP Connection drop count       : 19
    TCP TIME WAIT connection count  : 0

  Non Stop Routing:
    JSR Split failure count         : 0
    JSR Merge failure count         : 0
    JSR PRL Queue full count        : 0

NH Index Space Allocation
=========================================================
```

```
    Index_Space_type             Used        Available
            Reserved               64             1280
             Private               39              665
             Regular               60          1046466
           Extended                 0         15728638

Maximum possible number of private nexthops: 704
Percentage of private nexthop index space reserved for IRI:(internal routing) 30
Number of nexthop indices reserved for IRI:(internal routing) 212

Printing gencfg blobs statistics by major type

                                Type   Num Blobs   Data size
                      Proxy gencfg           33           0
                 L2 forwarding blob            1         128
                           COS BLOB           41       36996
                    Feature License            1           2
                           Firewall           21        4044
                            CH Info            1           0
              Libpeer PeerInfo blob            2        4392
                        Resync blob            4          44
                        MACSEC blob            1           8
                        Agentd blob            4        5888
                      RPD EVPN blob            1          52
                           LFM Blob            1           8
                              Total          111       51562
```

show system monitor memory events

Syntax

```
show system monitor memory events (all | system | process)
```

Release Information
Command introduced in Junos OS Release 20.1R1.

Description
Displays the history of events, whether they are major, minor, or critical. The events can be either for the system or per process. Use this command to view all the recorded events. When the condition is first detected, an event is raised. If the condition persists with the same severity, the event is not reported multiple times. However, if the condition persists with a changed severity or is detected after a reset, the event is reported again.

Options
all— Display the history of events for the entire system as well as per process.

system— Display the history of events at the system level.

process— Display the history of events per process.

Required Privilege Level
admin

RELATED DOCUMENTATION

show system monitor memory status | 3134

List of Sample Output
show system monitor memory events all on page 3132
show system monitor memory events process on page 3132
show system monitor memory events system on page 3133

Output Fields
Table 302 on page 3132 lists the output fields for the **show system monitor memory events** command. Output fields are listed in the approximate order in which they appear.

Table 302: show system monitor memory events Output Fields

Field Name	Field Description	Level of Output
Category	Specifies if the event is generated at the system level or at the process level.	**all** **process** **system**
Event	The Event that is raised when a threshold is crossed either at the system level or at the process level.	**all** **process** **system**
Type	Type of event. Values are: major, minor, and critical.	**all** **process** **system**
for process	Name of the process that has crossed the threshold value.	**all** **process**
with pid	Process identification number used to identify the process that crossed the threshold value.	**all** **process**

Sample Output

show system monitor memory events all

`user@host>` **show system monitor memory events all**

```
Feb 24 10:08:21 [system] Event: free_page_event Type minor
Feb 24 13:42:13 [process-threshold] Event: critical-event for process: xxxxx with
 pid xxxxx
Feb 24 17:15:32 [system] Event: free_page_event Type minor
Feb 25 11:47:50 [process-threshold] Event: critical-event for process: xxxxx with
 pid xxxxx
```

show system monitor memory events process

`user@host>` **show system monitor memory events process**

```
Feb 24 10:08:21 [system] Event: free_page_event Type minor
Feb 24 17:15:32 [system] Event: free_page_event Type minor
```

show system monitor memory events system

user@host> **show system monitor memory events system**

```
Feb 24 13:42:13 [process-threshold] Event: critical-event for process: xxxxx with
 pid xxxxx
Feb 25 11:47:50 [process-threshold] Event: critical-event for process: xxxxx with
 pid xxxxx
```

show system monitor memory status

Syntax

```
show system monitor memory status (all | system | process)
```

Release Information
Command introduced in Junos OS Release 20.1R1.

Description
Displays the current instant snapshot of the health of the device. You can view current health of both the modules: system and process.

Options
all— Display the memory usage status of the entire system as well as per process.

system— Display the memory usage status at the system level.

process— Display the memory usage status per process.

Required Privilege Level
admin

RELATED DOCUMENTATION

show system monitor memory events | 3131

List of Sample Output
show system monitor memory status all on page 3135
show system monitor memory status process on page 3135
show system monitor memory status system on page 3136

Output Fields
Table 302 on page 3132 lists the output fields for the **show system monitor memory** command. Output fields are listed in the approximate order in which they appear.

Table 303: show system monitor memory Output Fields

Field Name	Field Description	Level of Output
No.	Number	**all** **process**

Table 303: show system monitor memory Output Fields *(continued)*

Field Name	Field Description	Level of Output
Resource	Resource that is monitored. For instance, Cache and free pages, memory utilization at the kernel level, swap usage, and others.	**all** **system**
processID	The Process identification number of the process that has crossed the threshold value.	**all** **process**
processName	Name of the process that has crossed the threshold value.	**all** **process**
Alarm-Type	The type of alarm generated. Values are: major-event, minor-event, and critical-event.	**all** **process**
Event-Type	The type of event raised. Values are: major-event, minor-event, and critical-event.	**all** **system**

Sample Output

show system monitor memory status all

`user@host>` **show system monitor memory status all**

```
-----------------------------------------------
No.      (processID, processName)  Alarm-Type
-----------------------------------------------
1.       ('xxxxx', 'xxxxx')        critical-event
-----------------------------------------
Resource                      Event-Type
-----------------------------------------
Free pages:                   minor-event
```

show system monitor memory status process

`user@host>` **show system monitor memory status process**

```
-----------------------------------------------
No.      (processID, processName)  Alarm-Type
```

```
-----------------------------------------------
1.       ('xxxxx', 'xxxxx')        critical-event
```

show system monitor memory status system

user@host> **show system monitor memory status system**

```
-------------------------------------------
Resource                      Event-Type
-------------------------------------------
Free pages:                   minor-event
```

show system monitor memory actions

Syntax

```
show system monitor memory actions (all | system | process)
```

Release Information

Command introduced in Junos OS Release 20.2R1

Description

Displays the history of actions performed when the threshold level for any event is crossed. You can view the history of actions for a process or for a system or both.

Options

all—Display the history of actions performed when the threshold level for any event is crossed for the entire system as well as per process.

system—Display the history of actions performed when the threshold level for any event is crossed at the system level.

process—Display the history of actions performed when the threshold level for any event is crossed at the process level.

Required Privilege Level

admin

List of Sample Output

show system monitor memory actions all on page 3138
show system monitor memory actions process on page 3138

Output Fields

Table 304 on page 3137 lists the output fields for the **show system monitor memory actions** command. Output fields are listed in the approximate order in which they appear.

Table 304: show system monitor memory action Output Fields

Field Name	Field Description	Level of Output
Category	Specifies if the action is generated at the system level or at the process level.	**all** **process** **system**
process	Name of the process that has crossed the threshold value and process identification number used to identify the process that crossed the threshold value.	**all** **process**

Table 304: show system monitor memory action Output Fields *(continued)*

Field Name	Field Description	Level of Output
Action	The actions performed when a threshold is crossed either at the system level or at the process level.	**all** **process** **system**

Sample Output

show system monitor memory actions all

```
user@host> show system monitor memory actions all
```

```
May 08 10:56:00 [process-action]: process: ('xxxxx', 'xxx') action: snmp-trap
May 08 10:56:02 [process-action]: process: ('xxxxx', 'xxx') action: snmp-trap
```

show system monitor memory actions process

```
user@host> show system monitor memory actions process
```

```
May 08 10:56:00 [process-action]: process: ('11727', 'dcd') action: snmp-trap
May 08 10:56:02 [process-action]: process: ('11716', 'jkhmd') action: snmp-trap
```

show system resource-monitor fpc

Syntax

```
show system resource-monitor fpc
<slot slot-number>
```

Release Information

Command introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.
Command introduced in Junos OS Release 16.1 for EX9200 switches.

Description

Display the utilization of memory resources on the Packet Forwarding Engines for all FPCs or a specific FPC. The filter memory denotes the filter counter memory used for firewall filter counters. The asterisk (*) displayed next to each of the memory regions denotes the ones for which the configured threshold is being currently exceeded.

Options

slot *slot-number*—Display the Junos OS utilization information of memory resources for the specified slot number in which the FPC (or MPC) is installed.

NOTE: On the MX80 router, the MPCs are built into the chassis and are represented in the CLI as either **FPC 0** or **FPC 1**. This command supports only FPC 1 for the MX80 router.

Additional Information

The filter memory denotes the filter counter memory used for firewall filter counters. From the Ukern perspective, MPC5E contains only one Packet Forwarding Engine instance. The **show chassis fabric plane** command output displays the state of fabric plane connections to the Packet Forwarding Engine. Because two Packet Forwarding Engines exist, you notice PFE-0 and PFE-1 in the output.

Required Privilege Level

view

RELATED DOCUMENTATION

- *show system resource-monitor summary*
- *show system resource-monitor ifd-cos-queue-mapping fpc*
- *show system resource-monitor subscribers-limit*

List of Sample Output

show system resource-monitor fpc (All Slots) on page 3140
show system resource-monitor fpc (Specific Slot) on page 3141

Output Fields

Table 305 on page 3140 lists the output fields for the **show system resource-monitor fpc** command. Output fields are listed in the approximate order in which they appear.

Table 305: show system resource-monitor fpc Output Fields

Field Name	Field Description
Free Heap Memory Watermark	Configured watermark value for the percentage of free memory space used for ukernel or heap memory to be monitored
Free FW Memory Watermark	Configured watermark value for the percentage of free memory space used for firewall or filter memory to be monitored
Free NH Memory Watermark	Configured watermark value for the percentage of free memory space used for next-hop memory to be monitored
* **- watermark reached**	An asterisk (*) displayed beside any of the memory regions denotes the memory types for which the configured threshold is being currently exceeded.
Slot #	Slot number in which the line card is installed
PFE #	Number or identifier of the Packet Forwarding Engine in the specified line card slot
Heap % free	Percentage of free space associated with heap or ukernel memory
Encap mem % free	Percentage of free space associated with encapsulation memory
NH mem % free	Percentage of free space associated with next-hop memory
Filter / FW mem % free	Percentage of free space associated with firewall or filter memory

Sample Output

show system resource-monitor fpc (All Slots)

```
show system resource-monitor fpc
```

```
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached


Slot #         % Heap Free        RTT      Average RTT
     0             89               103     102(30)

                 PFE #      % ENCAP mem Free      % NH mem Free      % FW mem Free

                     0             NA                 78                 99

Slot #         % Heap Free        RTT      Average RTT
     2             88               103     103(30)

                 PFE #      % ENCAP mem Free      % NH mem Free      % FW mem Free

                     0             NA                 80                 99
                     1             NA                 80                 99

Slot #         % Heap Free        RTT      Average RTT
     3             91                 0      --(--)

                 PFE #      % ENCAP mem Free      % NH mem Free      % FW mem Free

                     0             99                 82                 72
                     1             99                 82                 72
```

show system resource-monitor fpc (Specific Slot)

```
show system resource-monitor fpc slot 2
```

```
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached
```

```
Slot #          % Heap Free         RTT       Average RTT
     2              88                 103      103(30)

                  PFE #      % ENCAP mem Free      % NH mem Free      % FW mem Free

                     0              NA                 80                 99
                     1              NA                 80                 99
```