# Network Management and Monitoring Feature Guide for EX2300, EX3400, and EX4300 Switches

Release
16.1

Modified: 2016-12-07

Copyright © 2016, Juniper Networks, Inc.

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

*Network Management and Monitoring Feature Guide for EX2300, EX3400, and EX4300 Switches*
Release 16.1
Copyright © 2016, 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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents


About the Documentation . . . . . xvii
Documentation and Release Notes . . . . . xvii
Supported Platforms . . . . . xvii
Using the Examples in This Manual . . . . . xvii
Merging a Full Example . . . . . xviii
Merging a Snippet . . . . . xviii
Documentation Conventions . . . . . xix
Documentation Feedback . . . . . xxi
Requesting Technical Support . . . . . xxi
Self-Help Online Tools and Resources . . . . . xxi
Opening a Case with JTAC . . . . . xxii

Part 1 Network Management and Monitoring

Chapter 1 Configuring Real-Time Performance Monitoring . . . . . 3

Understanding Real-Time Performance Monitoring on EX Series Switches . . . . . 4
RPM Packet Collection . . . . . 4
Tests and Probe Types . . . . . 4
Hardware Timestamps . . . . . 5
Limitations of RPM on EX Series Switches . . . . . 7
Configuring Real-Time Performance Monitoring (J-Web Procedure) . . . . . 7
Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) . . . . . 14
Viewing Real-Time Performance Monitoring Information . . . . . 16

Chapter 2 Configuring Analyzers and Port Mirroring . . . . . 17

Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches . . . . . 18
Port Mirroring Overview . . . . . 18
Analyzer Overview . . . . . 19
Port Mirroring and Analyzer Terminologies . . . . . 19
Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches . . . . . 21
Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches . . . . . 23
Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches . . . . . 30


Copyright © 2016, Juniper Networks, Inc.

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches . . . 40
Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) . . . 47
Configuring an Analyzer for Local Traffic Analysis . . . 48
Configuring an Analyzer for Remote Traffic Analysis . . . 48
Configuring Port Mirroring . . . 49
Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) . . . 50
Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches . . . 53
Troubleshooting Port Mirroring Configuration Error Messages . . . 54
An Analyzer Configuration Returns a "Multiple interfaces cannot be configured as a member of Analyzer output VLAN" Error Message . . . 54

Chapter 3 **Configuring sFlow Monitoring Technology . . . 57**

Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch . . . 57
Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches . . . 57
Adaptive Sampling . . . 58
sFlow Agent Address Assignment . . . 59
Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches . . . 60
Configuring sFlow Technology for Network Monitoring (CLI Procedure) . . . 64

Chapter 4 **Configuring Ethernet OAM Link Fault Management and Connectivity Fault Management . . . 67**

Understanding Ethernet OAM Link Fault Management for an EX Series Switch . . . 67
Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch . . . 69
Understanding Ethernet Frame Delay Measurements on Switches . . . 70
Ethernet Frame Delay Measurements . . . 70
Types of Ethernet Frame Delay Measurements . . . 71
Limitations . . . 72
Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches . . . 72
Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches . . . 76
Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) . . . 79
Creating the Maintenance Domain . . . 79
Configuring the Maintenance Domain MIP Half Function . . . 80
Creating a Maintenance Association . . . 80
Configuring the Continuity Check Protocol . . . 80
Configuring a Maintenance Association End Point . . . 81
Configuring a Connectivity Fault Management Action Profile . . . 82
Configuring the Linktrace Protocol . . . 82
Configuring Ethernet OAM Link Fault Management (CLI Procedure) . . . 83


Copyright © 2016, Juniper Networks, Inc.

Chapter 5 Configuring Uplink Failure Detection . . . . . 85
Understanding Uplink Failure Detection . . . . . 85
Uplink Failure Detection Overview . . . . . 85
Failure Detection Pair . . . . . 86
Configuring Interfaces for Uplink Failure Detection (CLI Procedure) . . . . . 87
Verifying That Uplink Failure Detection Is Working Correctly . . . . . 88
Chapter 6 Configuring Network Analytics . . . . . 89
Network Analytics Overview . . . . . 89
Analytics Feature Overview . . . . . 90
Network Analytics Enhancements Overview . . . . . 91
Summary of CLI Changes . . . . . 92
Understanding Enhanced Network Analytics Streaming Data . . . . . 97
Google Protocol Buffer (GPB) . . . . . 97
JavaScript Object Notation (JSON) . . . . . 99
Comma-separated Values (CSV) . . . . . 100
Tab-separated Values (TSV) . . . . . 100
Queue Statistics Output for JSON, CSV, and TSV . . . . . 100
Traffic Statistics Output for JSON, CSV, and TSV . . . . . 101
Understanding Enhanced Analytics Local File Output . . . . . 102
Prototype File for the Google Protocol Buffer Stream Format . . . . . 104
Example: Configuring Enhanced Network Analytics Features . . . . . 105
Configuring Queue Monitoring . . . . . 115
Configuring Traffic Monitoring . . . . . 117
Configuring a Local File for Network Analytics Data . . . . . 118
Configuring a Remote Collector for Streaming Analytics Data . . . . . 119
Chapter 7 Configuring SNMP . . . . . 121
Configuring SNMP (J-Web Procedure) . . . . . 121
Configuring the Local Engine ID . . . . . 124
Chapter 8 Monitoring and Troubleshooting . . . . . 127
Monitoring Hosts Using the J-Web Ping Host Tool . . . . . 127
Monitoring Network Traffic Using Traceroute . . . . . 129
Part 2 Configuration Statements
Chapter 9 Realtime Performance Monitoring . . . . . 133
data-fill . . . . . 134
data-size . . . . . 135
destination-port . . . . . 136
dscp-code-point . . . . . 137
hardware-timestamp . . . . . 138
history-size . . . . . 139
moving-average-size . . . . . 140
one-way-hardware-timestamp . . . . . 140
port (RPM) . . . . . 141
probe . . . . . 142
probe-count . . . . . 143
probe-interval . . . . . 144

Copyright © 2016, Juniper Networks, Inc. 

probe-limit . . . 145
probe-server . . . 146
probe-type . . . 147
routing-instance . . . 148
routing-instances . . . 149
rpm (Interfaces) . . . 150
source-address (Services) . . . 151
tcp . . . 152
test . . . 153
test-interval . . . 154
thresholds . . . 155
traps . . . 157
udp . . . 158

Chapter 10 Analyzers and Port Mirroring . . . 159

egress . . . 159
egress (Analyzer) . . . 160
ingress (vlans) . . . 160
ingress (Analyzer) . . . 161
input (Analyzer) . . . 162
interface (Analyzer) . . . 163
no-tag . . . 164
output (Mirroring) . . . 165
vlan (Mirroring) . . . 166

Chapter 11 sFlow Monitoring Technology . . . 167

agent-id . . . 167
collector . . . 168
disable (sFlow Monitoring Technology) . . . 168
interfaces (sFlow Monitoring Technology) . . . 169
polling-interval . . . 170
sample-rate . . . 171
sflow . . . 172
source-ip . . . 173
udp-port . . . 173

Chapter 12 Ethernet OAM Link Fault Management and Connectivity Fault Management . . . 175

action-profile (Applying to OAM CFM, for EX Series Switch Only) . . . 177
age (EX Series Switch Only) . . . 178
auto-discovery (EX Series Switch Only) . . . 178
calculation-weight . . . 179
connectivity-fault-management (EX Series Switch Only) . . . 180
continuity-check (EX Series Switch Only) . . . 181
cycle-time . . . 182
delay . . . 183
delay-variation . . . 184
direction (EX Series Switch Only) . . . 185
hold-interval (OAM CFM, for EX Series Switch Only) . . . 185
interface (OAM CFM, for EX Series Switch Only) . . . 186


Copyright © 2016, Juniper Networks, Inc.

interval (EX Series Switch Only) . . . 187
iteration-period . . . 188
level (EX Series Switch Only) . . . 188
linktrace (EX Series Switch Only) . . . 189
loss-threshold (EX Series Switch Only) . . . 189
maintenance-association (EX Series Switch Only) . . . 190
maintenance-domain (EX Series Switch Only) . . . 191
measurement-type (OAM LFM) . . . 192
mep (EX Series Switch Only) . . . 193
mip-half-function (EX Series Switch Only) . . . 194
name-format (EX Series Switch Only) . . . 195
path-database-size (EX Series Switch Only) . . . 195
performance-monitoring (OAM LFM) . . . 196
remote-mep (EX Series Switch Only) . . . 197
sla-iterator-profiles (OAM LFM) . . . 198
action (OAM LFM) . . . 198
action-profile . . . 199
allow-remote-loopback . . . 200
ethernet (OAM LFM) . . . 201
event (OAM LFM) . . . 204
event-thresholds . . . 204
frame-error . . . 205
frame-period . . . 205
frame-period-summary . . . 206
interface (OAM LFM) . . . 207
link-adjacency-loss . . . 208
link-discovery . . . 208
link-down . . . 209
link-event-rate . . . 209
link-fault-management . . . 210
negotiation-options . . . 211
no-allow-link-events . . . 211
oam . . . 212
pdu-interval . . . 214
pdu-threshold . . . 215
remote-loopback . . . 215
symbol-period . . . 216
syslog (OAM LFM) . . . 216

Chapter 13 **Uplink Failure Detection . . . 217**

action (Uplink Failure Detection) . . . 217
group (Uplink Failure Detection) . . . 218
link-to-disable . . . 218
link-to-monitor . . . 219
traceoptions (Uplink Failure Detection) . . . 220
uplink-failure-detection . . . 221

Chapter 14 **Network Analytics . . . 223**

address (Analytics Collector) . . . 224
analytics . . . 225

Copyright © 2016, Juniper Networks, Inc.

collector (Analytics) . . . 229
depth-threshold . . . 230
export-profiles . . . 231
file (Analytics) . . . 233
interface (Export Profiles) . . . 235
interfaces (Analytics Resource) . . . 236
latency-threshold . . . 237
local (Analytics Collector) . . . 238
resource (Analytics) . . . 239
resource-profiles (Analytics) . . . 240
system (Analytics Resource) . . . 241
system (Export Profiles) . . . 242
traceoptions (Analytics) . . . 243

Chapter 15 SNMP . . . 245

address . . . 248
address-mask . . . 248
agent-address . . . 249
alarm (SNMP RMON) . . . 250
authorization . . . 251
bucket-size . . . 251
categories . . . 252
client-list . . . 252
client-list-name . . . 253
clients . . . 253
commit-delay . . . 254
community (SNMP) . . . 255
community . . . 256
community-name . . . 257
contact (SNMP) . . . 258
description . . . 258
description . . . 259
destination-port . . . 259
engine-id . . . 260
event . . . 261
falling-event-index . . . 261
falling-threshold . . . 262
falling-threshold . . . 263
falling-threshold-interval . . . 264
filter-duplicates . . . 264
filter-interfaces . . . 265
group (Configuring Group Name) . . . 266
group (Defining Access Privileges for an SNMPv3 Group) . . . 267
health-monitor . . . 267
history . . . 268
interface (SNMP RMON History) . . . 269
interface (SNMP) . . . 269
interval . . . 270
interval . . . 270


Copyright © 2016, Juniper Networks, Inc.

interval . . . 271
location (SNMP) . . . 271
logical-system . . . 272
message-processing-model . . . 273
name . . . 273
nonvolatile . . . 274
notify . . . 275
notify-filter (Applying to the Management Target) . . . 276
notify-filter (Configuring the Profile Name) . . . 276
notify-view . . . 277
oid . . . 277
oid . . . 278
owner . . . 278
parameters . . . 279
port . . . 279
read-view . . . 280
request-type . . . 281
rising-event-index . . . 282
rising-threshold . . . 283
rising-threshold . . . 284
rmon . . . 284
rmon . . . 285
routing-instance . . . 286
routing-instance . . . 287
sample-type . . . 287
security-level (Defining Access Privileges) . . . 288
security-level (Generating SNMP Notifications) . . . 289
security-model (Access Privileges) . . . 290
security-model (Group) . . . 291
security-model (SNMP Notifications) . . . 291
security-name (Security Group) . . . 292
security-name (Community String) . . . 293
security-name (SNMP Notifications) . . . 294
security-to-group . . . 295
snmp . . . 295
snmp . . . 296
snmp-community . . . 296
source-address . . . 297
startup-alarm . . . 298
syslog-subtag . . . 298
tag . . . 299
tag-list . . . 299
target-address . . . 300
target-parameters . . . 301
targets . . . 302
traceoptions (SNMP) . . . 303
trap-group . . . 305
trap-options . . . 306
type . . . 307

Copyright © 2016, Juniper Networks, Inc. 

type . . . 308
v3 . . . 309
vacm . . . 311
variable . . . 312
version (SNMP) . . . 312
view (Associating a MIB View with a Community) . . . 313
view (Configuring a MIB View) . . . 314
write-view . . . 315

Part 3 Operational Commands

Chapter 16 Realtime Performance Monitoring . . . 319

show services rpm active-servers . . . 320
show services rpm history-results . . . 321
show services rpm probe-results . . . 324

Chapter 17 General Commands . . . 331

monitor traffic . . . 332
ping . . . 344
show pfe statistics bridge . . . 348
traceroute . . . 353

Chapter 18 Analyzers and Port Mirroring . . . 357

show analyzer . . . 358

Chapter 19 sFlow Monitoring Technology . . . 361

show sflow . . . 362
show sflow interface . . . 364
show sflow collector . . . 366
clear sflow collectors statistics . . . 367

Chapter 20 Ethernet OAM Connectivity Fault Management . . . 369

clear oam ethernet connectivity-fault-management delay-statistics . . . 370
clear oam ethernet connectivity-fault-management sla-iterator-statistics . . . 372
clear oam ethernet connectivity-fault-management statistics . . . 373
monitor ethernet delay-measurement . . . 374
show oam ethernet connectivity-fault-management delay-statistics . . . 379
show oam ethernet connectivity-fault-management forwarding-state . . . 383
show oam ethernet connectivity-fault-management interfaces . . . 387
show oam ethernet connectivity-fault-management path-database . . . 393
show oam ethernet connectivity-fault-management mep-database . . . 396
show oam ethernet connectivity-fault-management mip . . . 402
show oam ethernet connectivity-fault-management sla-iterator-statistics . . . 403

Chapter 21 Ethernet OAM Link Fault Management . . . 409

show oam ethernet link-fault-management . . . 410

Chapter 22 Uplink Failure Detection . . . 415

show uplink-failure-detection . . . 416


Copyright © 2016, Juniper Networks, Inc.

Chapter 23 SNMP . . . . . 419

clear snmp rmon history . . . . . 420
clear snmp statistics . . . . . 421
request snmp spoof-trap . . . . . 423
show snmp health-monitor . . . . . 429
show snmp inform-statistics . . . . . 436
show snmp mib . . . . . 438
show snmp rmon . . . . . 441
show snmp rmon history . . . . . 445
show snmp statistics . . . . . 449
show snmp v3 . . . . . 457

Copyright © 2016, Juniper Networks, Inc. 

Copyright © 2016, Juniper Networks, Inc.

# List of Figures


Part 1 Network Management and Monitoring

Chapter 1 **Configuring Real-Time Performance Monitoring . . . . . 3**

Figure 1: RPM Timestamps . . . . . 6

Chapter 2 **Configuring Analyzers and Port Mirroring . . . . . 17**

Figure 2: Network Topology for Local Mirroring Example . . . . . 25
Figure 3: Remote Mirroring Network Topology Example . . . . . 31
Figure 4: Remote Mirroring Through a Transit Switch Network–Sample Topology . . . . . 41

Chapter 3 **Configuring sFlow Monitoring Technology . . . . . 57**

Figure 5: sFlow Technology Monitoring System . . . . . 61

Chapter 4 **Configuring Ethernet OAM Link Fault Management and Connectivity Fault Management . . . . . 67**

Figure 6: Relationship Among MEPs, MIPs, and Maintenance Domain Levels . . . 70

Chapter 5 **Configuring Uplink Failure Detection . . . . . 85**

Figure 7: Uplink Failure Detection Configuration on Switches . . . . . 86


Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

# List of Tables


About the Documentation . . . . . xvii

Table 1: Notice Icons . . . . . xix
Table 2: Text and Syntax Conventions . . . . . xix

Part 1 Network Management and Monitoring

Chapter 1 Configuring Real-Time Performance Monitoring . . . . . 3

Table 3: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields . . . . . 9
Table 4: Performance Probe Tests Configuration Fields . . . . . 10

Chapter 2 Configuring Analyzers and Port Mirroring . . . . . 17

Table 5: Mirroring Terminologies . . . . . 19
Table 6: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches . . . . . 21
Table 7: Port Mirroring Configuration Settings . . . . . 51

Chapter 6 Configuring Network Analytics . . . . . 89

Table 8: Network Analytics CLI Changes . . . . . 92
Table 9: GPB Stream Format Message Header Information . . . . . 97
Table 10: Streamed Queue Statistics Data Output Fields . . . . . 101
Table 11: Streamed Traffic Statistics Data Output Fields . . . . . 101
Table 12: Output Fields for Queue Statistics in Local Analytics File . . . . . 103
Table 13: Output Fields for Traffic Statistics in Local Analytics File . . . . . 103

Chapter 7 Configuring SNMP . . . . . 121

Table 14: SNMP Configuration Page . . . . . 121

Chapter 8 Monitoring and Troubleshooting . . . . . 127

Table 15: J-Web Ping Host Field Summary . . . . . 127
Table 16: Traceroute field summary . . . . . 129

Part 3 Operational Commands

Chapter 16 Realtime Performance Monitoring . . . . . 319

Table 17: show services rpm active-servers Output Fields . . . . . 320
Table 18: show services rpm history-results Output Fields . . . . . 321
Table 19: show services rpm probe-results Output Fields . . . . . 324

Chapter 17 General Commands . . . . . 331

Table 20: Match Conditions for the monitor traffic Command . . . . . 334
Table 21: Logical Operators for the monitor traffic Command . . . . . 336


Copyright © 2016, Juniper Networks, Inc.

Table 22: Arithmetic and Relational Operators for the monitor traffic Command . . . 337
Table 23: show pfe statistics bridge Output Fields . . . 348
Table 24: traceroute Output Fields . . . 355

Chapter 18 Analyzers and Port Mirroring . . . 357

Table 25: show analyzer Output Fields . . . 358

Chapter 19 sFlow Monitoring Technology . . . 361

Table 26: show sflow Output Fields . . . 362
Table 27: show sflow interface Output Fields . . . 364
Table 28: show sflow collector Output Fields . . . 366

Chapter 20 Ethernet OAM Connectivity Fault Management . . . 369

Table 29: monitor ethernet delay-measurement one-way Output Fields . . . 376
Table 30: monitor ethernet delay-measurement two-way Output Fields . . . 376
Table 31: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields . . . 380
Table 32: show oam ethernet connectivity-fault-management forwarding-state Output Fields . . . 383
Table 33: show oam ethernet connectivity-fault-management interfaces Output Fields . . . 387
Table 34: show oam ethernet connectivity-fault-management linktrace path-database Output Fields . . . 393
Table 35: show oam ethernet connectivity-fault-management mep-database Output Fields . . . 396
Table 36: show oam ethernet connectivity-fault-management mip Output Fields . . . 402
Table 37: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields . . . 403

Chapter 21 Ethernet OAM Link Fault Management . . . 409

Table 38: show oam ethernet link-fault-management Output Fields . . . 410

Chapter 22 Uplink Failure Detection . . . 415

Table 39: show uplink-failure-detection Output Fields . . . 416

Chapter 23 SNMP . . . 419

Table 40: show snmp health-monitor Output Fields . . . 429
Table 41: show snmp inform-statistics Output Fields . . . 436
Table 42: show snmp mib Output Fields . . . 439
Table 43: show snmp rmon Output Fields . . . 441
Table 44: show smp rmon history Output Fields . . . 445
Table 45: show snmp statistics Output Fields . . . 450
Table 46: show snmp statistics subagents Output Fields . . . 453
Table 47: show snmp v3 Output Fields . . . 458


Copyright © 2016, Juniper Networks, Inc.

# About the Documentation


- Documentation and Release Notes on page xvii
- Supported Platforms on page xvii
- Using the Examples in This Manual on page xvii
- Documentation Conventions on page xix
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxi


## 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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

## Supported Platforms

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

- EX Series

## 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.

Copyright © 2016, Juniper Networks, Inc.

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:


Copyright © 2016, Juniper Networks, Inc.

```
[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 xix 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 xix 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:<br><br>user@host> **configure** |

Copyright © 2016, Juniper Networks, Inc.

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

| Convention | Description | Examples |
|---|---|---|
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host>` **show chassis alarms**<br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies guide names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS CLI User Guide*<br>• RFC 1997, *BGP Communities Attribute* |
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br>[edit]<br>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.<br>• 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**<br>**(*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]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| GUI Conventions | | |
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select **All Interfaces**.<br>• To cancel the configuration, click **Cancel**. |


Copyright © 2016, Juniper Networks, Inc.

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

| Convention | Description | Examples |
|---|---|---|
| > (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, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/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 J-Care or Partner Support Service 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

Copyright © 2016, Juniper Networks, Inc.

- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

## Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- 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 http://www.juniper.net/support/requesting-support.html.


Copyright © 2016, Juniper Networks, Inc.

PART 1

# Network Management and Monitoring


- Configuring Real-Time Performance Monitoring on page 3
- Configuring Analyzers and Port Mirroring on page 17
- Configuring sFlow Monitoring Technology on page 57
- Configuring Ethernet OAM Link Fault Management and Connectivity Fault Management on page 67
- Configuring Uplink Failure Detection on page 85
- Configuring Network Analytics on page 89
- Configuring SNMP on page 121


Copyright © 2016, Juniper Networks, Inc.

 Copyright © 2016, Juniper Networks, Inc.

CHAPTER 1

# Configuring Real-Time Performance Monitoring


- Understanding Real-Time Performance Monitoring on EX Series Switches on page 4
- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 7
- Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) on page 14
- Viewing Real-Time Performance Monitoring Information on page 16


Copyright © 2016, Juniper Networks, Inc.

# Understanding Real-Time Performance Monitoring on EX Series Switches

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 Ethernet 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 on page 4
- Tests and Probe Types on page 4
- Hardware Timestamps on page 5
- Limitations of RPM on EX Series Switches on page 7


## 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 switches support the following tests and probe types:

- Ping tests:


Copyright © 2016, Juniper Networks, Inc.

  - 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, then timers are generated at the software level and are less accurate than they would have been with hardware timestamps.

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

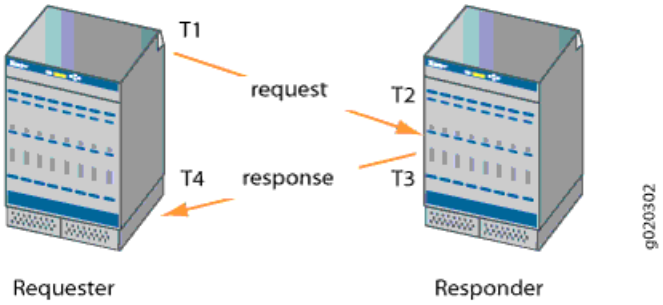
You should configure the requester (the RPM client) with hardware timestamps (see Figure 1 on page 6) to get more meaningful results than you would get without the timestamps.The responder (the RPM server) does not need to be configured to support hardware timestamps. If the responder supports hardware 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: Hardware timestamps are supported on all EX Series switches.

Figure 1 on page 6 shows the timestamps:

Copyright © 2016, Juniper Networks, Inc. 

Figure 1: 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

NOTE: See "Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure)" on page 14 for information on how to configure hardware timestamps on the requester.

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 1 on page 6, 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.


Copyright © 2016, Juniper Networks, Inc.

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 Switches

- Two-Way Active Measurement Protocol (TWAMP) is not supported on EX Series switches.
- EX Series 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.
  - EX Series switches do not support hardware timestamps for HTTP and TCP probes.
  - Timestamps apply only to IPv4 traffic.

**Related Documentation**

- For further details about RPM, see *Junos OS Services Interfaces Configuration Guide*
- Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) on page 14
- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 7
- Configuring SNMP (J-Web Procedure) on page 121
- Monitoring Network Traffic Using Traceroute on page 129

## Configuring Real-Time Performance Monitoring (J-Web Procedure)

NOTE: **This topic applies only to the J-Web Application package.**

Real-time performance monitoring (RPM) in EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. Jitter is the difference in relative transit time between two consecutive probes. You can set up probe owners and configure one or more performance probe tests under each probe owner.

The ways in which you can use RPM include:

Copyright © 2016, Juniper Networks, Inc.

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
- Set thresholds to trigger SNMP traps when threshold 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.
- Determine automatically whether a path exists between a host switch and its configured Border Gateway Protocol (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.

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.

EX Series switches support the following tests and probe types:

- Ping tests:
  - ICMP echo
  - ICMP timestamp
- HTTP tests:
  - HTTP get (not available for BGP RPM services)
- UDP and TCP tests with user-configured ports:
  - UDP echo
  - TCP connection
  - UDP timestamp

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You must configure both the requester and the responder to timestamp the RPM packets. The RPM features provides an additional configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way, rather than round-trip, times for packets to traverse the network between the requester and the responder.


Copyright © 2016, Juniper Networks, Inc.

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.
- If the responder does not support hardware timestamps, RPM can only report the round-trip measurements, it cannot calculate round-trip jitter.
- In EX Series switches timestamps apply only to IPv4 traffic.

To configure RPM using the J-Web interface:

1. Select **Troubleshoot** > **RPM** > **Configure RPM** .
2. In the **Configure RPM** page, enter information as specified in Table 3 on page 9.
   a. Click **Add** to set up the **Owner Name** and **Performance Probe Tests**.
   b. Select a probe owner from **Probe Owners** list and click **Delete** to remove the selected probe owner
   c. Double-click one of the probe owners in **Probe Owners** list to display the list of performance probe tests.
   d. Double-click one of the performance probe tests to edit the test parameters.
3. Enter the **Maximum Number of Concurrent Probes** and specify the **Probe Servers**.
4. Click **Apply** to apply the RPM probe settings.

### Table 3: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields

| Field | Function | Your Action |
|---|---|---|
| Probe Owners | Identifies a owner for whom 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. | 1. Click **Add** and type an owner name.<br>2. In **Performance Probe Tests**, click **Add** to define the RPM test parameters. See Table 4 on page 10 for information on configuring RPM test parameters.<br>3. Click **OK** to save the settings or **Cancel** to exit from the window without saving the changes. |
| Maximum Number of Concurrent Probes | Specifies the maximum number of concurrent probes allowed. | Type a number from 1 through 500. |

Copyright © 2016, Juniper Networks, Inc.

Table 3: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Probe Servers | Specifies the servers that act as receivers and transmitters for the probes. | Set up the following servers:<br>• TCP Probe Server—Specifies the port on which the device is to receive and transmit TCP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535.<br>• UDP Probe Server—Specifies the port on which the device is to receive and transmit UDP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535. |

Table 4: Performance Probe Tests Configuration Fields

| Field | Function | Your Action |
|---|---|---|
| Identification | | |
| Test Name | Identifies the RPM test. | Type a test name. |
| Target (Address or URL) | Specifies the IP address or the URL of the probe target. | Type the IP address in dotted decimal notation or the URL of the probe target. If the target is a URL, type a fully formed URL that includes **http://**. |
| Source Address | Specifies the IP address to be used as the probe source address. | Type the source address to be used for the probe. If you do not supply this value, the packet uses the outgoing interface's address as the probe source address. |
| Routing Instance | Specifies the routing instance over which the probe is sent. | Type the routing instance name. The routing instance applies only to **icmp-ping** and **icmp-ping-timestamp** probe types. The default routing instance is **inet.0**. |
| History Size | Specifies the number of probe results to be saved in the probe history. | Type a number from 0 through 255. The default history size is 50. |
| Request Information | | |


Copyright © 2016, Juniper Networks, Inc.

Table 4: Performance Probe Tests Configuration Fields *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Probe Type | Specifies the type of probe to send as part of the test. | Select a probe type from the list:<br>• **http-get**<br>• **http-get-metadata**<br>• **icmp-ping**<br>• **icmp-ping-timestamp**<br>• **tcp-ping**<br>• **udp-ping**<br>• **udp-ping-timestamp** |
| Interval | Sets the wait time (in seconds) between probe transmissions. | Type a number from 1 through 255 . |
| Test Interval | Sets the wait time (in seconds) between tests. | Type a number from 0 through 86400 . |
| Probe Count | Sets the total number of probes to be sent for each test. | Type a number from 1 through 15. |
| Moving Average Size | Specifies the number of samples to be used in the statistical calculation operations to be performed across a number of the most recent samples. | Type a number from 0 through 255. |
| Destination Port | Specifies the TCP or UDP port to which probes are sent.<br><br>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 network 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 49160 through 65535. |
| DSCP Bits | Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. | Type a valid 6-bit pattern. |
| Data Size | Specifies the size (in bytes) of the data portion of the ICMP probes. | Type a number from 0 through 65507. |
| Data Fill | Specifies the hexadecimal value of the data portion of the ICMP probes. | Type a hexadecimal value from 1h through 800h . |
| Hardware Timestamp | | |
| One Way Hardware Timestamp | Enables one-way hardware timestamp. | To enable timestamping, select the check box. |

Copyright © 2016, Juniper Networks, Inc.

Table 4: Performance Probe Tests Configuration Fields *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Destination Interface | Enables hardware timestamp on the specified interface. | Select an interface from the list. |
| **Maximum Probe Thresholds** | | |
| Successive Lost Probes | Sets the number of probes that can be lost successively, if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 15. |
| Lost Probes | Sets the number of probes that can be lost , if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 15. |
| Round Trip Time | Sets the round-trip time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Jitter | Sets the jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Standard Deviation | Sets the maximum allowable standard deviation (in microseconds), if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Egress Time | Sets the one-way time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Ingress Time | Sets the one-way time (in microseconds), from the remote server to the switch, if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000 (microseconds). |
| Jitter Egress Time | Sets the outbound-time jitter (in microseconds), if exceeded triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Jitter Ingress Time | Sets the inbound-time jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 and 60000000. |


Copyright © 2016, Juniper Networks, Inc.

Table 4: Performance Probe Tests Configuration Fields *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Egress Standard Deviation | Sets the maximum allowable standard deviation of outbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| Ingress Standard Deviation | Sets the maximum allowable standard deviation of inbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message. | Type a number from 0 through 60000000. |
| **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.<br>• 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.<br>• 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.<br>• To disable SNMP traps, clear the check box. |
| 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.<br>• 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.<br>• To disable SNMP traps, clear the check box. |
| Ingress Time Exceeded | Generates SNMP traps when the threshold for maximum inbound time is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |
| Jitter Exceeded | Generates SNMP traps when the threshold for jitter in round-trip time is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |

Copyright © 2016, Juniper Networks, Inc.

Table 4: Performance Probe Tests Configuration Fields *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Probe Failure | Generates SNMP traps when the threshold for the number of successive lost probes is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |
| RTT Exceeded | Generates SNMP traps when the threshold for maximum round-trip time is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |
| Standard Deviation Exceeded | Generates SNMP traps when the threshold for standard deviation in round-trip times is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |
| Test Completion | Generates SNMP traps when a test is completed. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |
| Test Failure | Generates SNMP traps when the threshold for the total number of lost probes is exceeded. | • To enable SNMP traps for this condition, select the check box.<br>• To disable SNMP traps, clear the check box. |

**Related Documentation**

- Configuring SNMP (J-Web Procedure) on page 121
- Viewing Real-Time Performance Monitoring Information on page 16

## Configuring the Interface for RPM Timestamping for Client/Server on an EX Series 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 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.

Timestamps apply only to IPv4 traffic.

You can enable hardware timestamps for the following RPM probe types:


Copyright © 2016, Juniper Networks, Inc.

- icmp-ping
- icmp-ping-timestamp
- udp-ping
- udp-ping-timestamp

To configure RPM probes and 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:

    ```
    [edit services rpm probe owner test test-name]
    user@switch# set hardware-timestamp
    ```

**Related Documentation**

- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 7

Copyright © 2016, Juniper Networks, Inc.

- Understanding Real-Time Performance Monitoring on EX Series Switches on page 4

## Viewing Real-Time Performance Monitoring Information

NOTE: This topic applies only to the J-Web Application package.

Real-time performance monitoring (RPM) on EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. The J-Web interface provides a graphical view of RPM information for EX Series switches.

To view the RPM information using the J-Web interface:

1. Select **Troubleshoot** >**RPM** >**View RPM**.
2. Select the **Round Trip Time** check box to display the graph with round-trip time included. Clear the check-box to view the graph without the round-trip time.
3. From the **Refresh Time** list, select a refresh time interval for the graph.

**Related Documentation**

- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 7


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 2

# Configuring Analyzers and Port Mirroring


- Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches on page 18
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 30
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches on page 40
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 47
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches on page 53
- Troubleshooting Port Mirroring Configuration Error Messages on page 54


Copyright © 2016, Juniper Networks, Inc.

# Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

NOTE: This concept uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

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.

Juniper Networks EX2300, EX3400, and EX4300 Ethernet Switches support the following mirroring methods: port mirroring and analyzers. You can use port mirroring or analyzers to facilitate analyzing traffic on these switches at the packet level. You might use analyzers 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.

Mirrored packets can be copied either to a local interface for local monitoring or to a VLAN for remote monitoring. The following packets can be copied:

- **Packets entering or exiting a port**—You can mirror the packets in any combination of packets entering or exiting ports on 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 a VLAN**—You can mirror the packets entering a VLAN 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 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. You can send the sample to a port-mirroring instance or to an analyzer VLAN.

This topic describes:


- Port Mirroring Overview on page 18
- Analyzer Overview on page 19
- Port Mirroring and Analyzer Terminologies on page 19
- Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches on page 21


## Port Mirroring Overview

You configure port mirroring on an EX2300, EX3400, or EX4300 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


Copyright © 2016, Juniper Networks, Inc.

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 either of the following ways:

- Implicitly reference the port-mirroring properties in effect on the port.
- Explicitly reference a particular named instance of port mirroring.

You can configure port mirroring at the **[edit forwarding-options port-mirroring]** hierarchy level.

NOTE: You can use port mirroring to mirror traffic on Layer 3 interfaces. Analyzers can be used to mirror bridged (Layer 2) packets. To mirror routed packets (Layer 3 packets), you can use the port mirroring configuration in which the family statement is set to inet or inet6.

## Analyzer Overview

You can configure an analyzer to define both the input traffic and output traffic in the same analyzer configuration. The input 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 and Analyzer Terminologies

Table 5 on page 19 lists some port mirroring terms and their descriptions.

### Table 5: Mirroring Terminologies

| Term | Description |
|---|---|
| Analyzer | In a mirroring configuration (analyzer) on an EX2300, EX3400, or EX4300 switch, the analyzer includes:<br>• The name of the analyzer<br>• Source (input) ports or VLAN<br>• A destination for mirrored packets (either a monitor port or a monitor VLAN) |

Copyright © 2016, Juniper Networks, Inc.

Table 5: Mirroring Terminologies *(continued)*

| Term | Description |
|---|---|
| Analyzer output interface<br><br>(Also known as monitor port) | Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected.<br><br>NOTE: Interfaces used as output for an analyzer must be configured under the **ethernet-switching** family.<br><br>Analyzer output interfaces have the following limitations:<br><br>• Cannot also be a source port.<br>• Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port-mirroring configuration.<br>• 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<br><br>(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. |
| 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<br><br>(Also known as mirrored ports or monitored interfaces) | An interface on the switch that is being mirrored. Traffic that is either 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 application. |
| Native analyzer session | An analyzer session that has both **input** and **output** definitions in its analyzer configuration. |
| Policy-based mirroring<br><br>(Also known as port 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. |


Copyright © 2016, Juniper Networks, Inc.

Table 5: Mirroring Terminologies *(continued)*

| Term | Description |
|---|---|
| Remote port mirroring | Functions the same way 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 or analyzers on EX2300, EX3400, and EX4300 switches, 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, which will enable mirroring on all interfaces. 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 6 on page 21 summarizes further configuration guidelines for mirroring on EX2300, EX3400, and EX4300 switches.

Table 6: 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 | |

Copyright © 2016, Juniper Networks, Inc.

Table 6: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches *(continued)*

| Guideline | Value or Support Information | Comment |
|---|---|---|
| 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:<br>  ◦ A maximum of four port-mirroring sessions (including the global port-mirroring session). See Table 5 on page 19 for a description of global port mirror.<br>  ◦ A maximum of four analyzer sessions.<br>  ◦ A combination of port-mirroring and analyzer sessions, and the total of this combination must be four.<br>• 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)<br>• Management Ethernet ports (**me0** or **vme0**)<br>• Integrated routing and bridging (IRB) interfaces; also known as routed VLAN interfaces (RVIs).<br>• VLAN-tagged Layer 3 interfaces | |
| Protocol families that you can include in a port-mirroring configuration for remote traffic. | **any** | |
| Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations. | Ingress only | |
| Mirrored packets exiting an interface reflect rewritten class-of-service (CoS) DSCP or 802.1p bits. | Applicable | |
| 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. |
| 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 | |


Copyright © 2016, Juniper Networks, Inc.

Table 6: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches *(continued)*

| Guideline | Value or Support Information | Comment |
|---|---|---|
| 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 | |

**Related Documentation**

- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 30
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 47

## Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches

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

Copyright © 2016, Juniper Networks, Inc.

You can analyze the mirrored traffic by using a protocol analyzer application installed on a system connected to the local destination interface (or running on 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 on page 24
- Overview and Topology on page 24
- Mirroring All Employee Traffic for Local Analysis on page 25
- Mirroring Employee-to-Web Traffic for Local Analysis on page 26
- Verification on page 28


## 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. For information about mirroring, see "Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches" on page 18.

## 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.

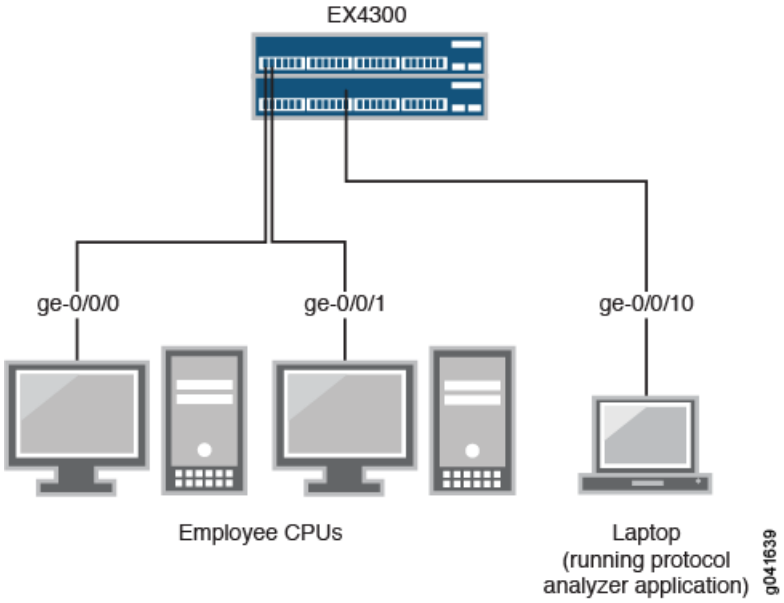
The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers. The interface ge0/0/10 is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.

NOTE: **Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.**

Both examples use the network topology shown in Figure 2 on page 25.


Copyright © 2016, Juniper Networks, Inc.

Figure 2: Network Topology for Local Mirroring Example




## Mirroring All Employee Traffic for Local Analysis

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]
user@swtich# set interfaces ge-0/0/0 unit 0 family ethernet-switching
user@switch# set interfaces ge-0/0/1 unit 0 family inet 192.0.2.1/24
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members
  analyzer_vlan
user@switch#  set vlans analyzer-vlan vlan-id 1000
user@switch# set forwarding-options analyzer employee–monitor input ingress interface
  ge-0/0/0.0
user@switch# set forwarding-options analyzer employee–monitor input ingress interface
  ge-0/0/1.0
user@switch# 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@swtitch# set analyzer (Port Mirroring) employee-monitor input ingress interface
     ge–0/0/0.0
   user@swtich# 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

Copyright © 2016, Juniper Networks, Inc.

```
[edit forwarding-options]
user@switch# set interfaces 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

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]
user@switch# set forwarding-options port-mirroring instance employee–web–monitor
  output interface ge-0/0/10.0
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-mirroring-instance employee-web-monitor
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input
  watch-employee
```


Copyright © 2016, Juniper Networks, Inc.

```
user@switch# 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;
            }
          }
        }
      }
```

Copyright © 2016, Juniper Networks, Inc.

```
    }
  }
  ...
  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

To confirm that the configuration is correct, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 28
- Verifying That The Port-Mirroring Instance Is Configured Properly on page 29

### 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.


Copyright © 2016, Juniper Networks, Inc.

**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 on page 30

Copyright © 2016, Juniper Networks, Inc.

- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 47
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches on page 18

## Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches

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 30. 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 on page 31
- Overview and Topology on page 31


Copyright © 2016, Juniper Networks, Inc.

- Mirroring All Employee Traffic for Remote Analysis on page 32
- Mirroring Employee-to-Web Traffic for Remote Analysis on page 35
- Verification on page 39


## 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:

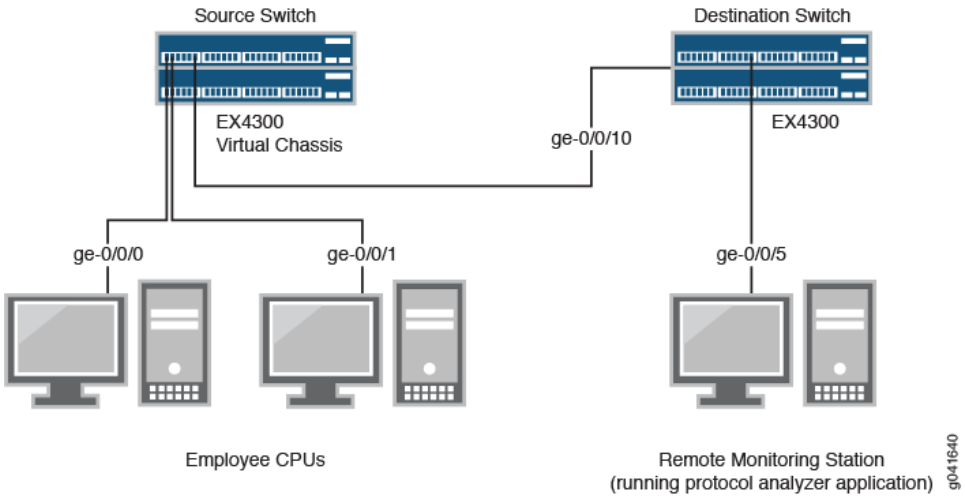
- You have an understanding of mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

## 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 3 on page 31 shows the network topology for both these example scenarios.

### Figure 3: 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
     ```

 Copyright © 2016, Juniper Networks, Inc.

```
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 {
```

Copyright © 2016, Juniper Networks, Inc.

```
        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;
```


Copyright © 2016, Juniper Networks, Inc.

```
        }
      }
      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
```

Copyright © 2016, Juniper Networks, Inc.

**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]
     ```


Copyright © 2016, Juniper Networks, Inc.

```
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 {
```


Copyright © 2016, Juniper Networks, Inc.

```
    input {
      ingress {
        vlan remote-analyzer;
      }
    }
    output {
      interface {
        ge-0/0/5.0;
      }
    }
  }
}
```

## Verification

To confirm that the configuration is working properly, perform these tasks:


- Verifying That the Analyzer Has Been Correctly Created on page 39


### 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.

Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 47
- Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches on page 18

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

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 Remote Monitoring of Employee Resource Use Through a Transit Switch 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 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 on page 41
- Overview and Topology on page 41


Copyright © 2016, Juniper Networks, Inc.

- Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch on page 42
- Verification on page 46


## 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.

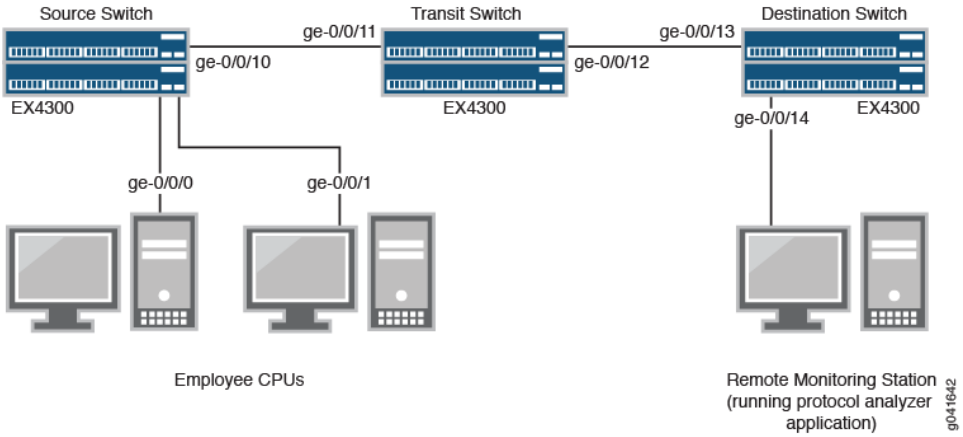
## Overview and Topology

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 4 on page 41 shows the network topology for this example.

### Figure 4: 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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
     ```

Copyright © 2016, Juniper Networks, Inc.

```
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]
```

 Copyright © 2016, Juniper Networks, Inc.

```
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;
```

Copyright © 2016, Juniper Networks, Inc.

```
        }
      }
    }
  }
  forwarding-options {
    analyzer employee-monitor {
      input {
        ingress {
          vlan remote-analyzer;
        }
      }
      output {
        interface {
          ge-0/0/14.0;
        }
      }
    }
  }
```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 46

### 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**.


Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 30
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 47
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches on page 18

## Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure)

NOTE: This task 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 *Configuring Port Mirroring to Analyze Traffic (CLI Procedure)*. 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

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.

Copyright © 2016, Juniper Networks, Inc.

NOTE: Interfaces used as output for an analyzer must be configured under the ethernet-switching family.


- Configuring an Analyzer for Local Traffic Analysis on page 48
- Configuring an Analyzer for Remote Traffic Analysis on page 48
- Configuring Port Mirroring on page 49


## 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
   ```


Copyright © 2016, Juniper Networks, Inc.

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 to which you will connect the computer running the protocol analyzer application:

      ```
      [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]
      ```

Copyright © 2016, Juniper Networks, Inc.

```
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 Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 30
- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- *Understanding Port Mirroring on EX Series Switches*
- *Firewall Filters for EX Series Switches Overview*

## Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.


Copyright © 2016, Juniper Networks, Inc.

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, EX4300, EX4500, EX6200 switches
- Packets exiting a VLAN on EX8200 switches

To configure port mirroring on an EX Series switch using the J-Web interface:

1. Select **Configure** > **Security** > **Port Mirroring**.

   The top of the screen displays analyzer details such as the name, status, analyzer port, ratio, and loss priority.

   The bottom of the screen lists ingress and egress ports of the selected analyzer.

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

2. Click one of the following options:
   - Add—Add an analyzer. Enter information as specified in Table 7 on page 51.
   - Edit—Modify details of the selected analyzer. Enter information as specified in Table 7 on page 51.
   - Delete—Delete the selected analyzer.
   - Enable/Disable—Enable or disable the selected analyzer (toggle).

   NOTE: On EX2200, EX3200, EX4200, and EX4500 switches, only one analyzer can be enabled at a time. On EX8200 switches, a maximum of seven analyzers can be enabled. On EX4300 switches a maximum of four Analyzers/Port Mirror instances can be enabled.

   NOTE: When an analyzer is deleted or disabled, any filter association is removed.

Table 7: Port Mirroring Configuration Settings

| Field | Function | Your Action |
|---|---|---|
| Analyzer Name | Specifies the name of the analyzer. | Type a name for the analyzer. |

Copyright © 2016, Juniper Networks, Inc.

Table 7: Port Mirroring Configuration Settings *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Ratio<br><br>NOTE: This option is not supported on EX4300 switches. | Specifies the ratio of packets to be mirrored. For example:<br>• A ratio of 1 sends copies of all packets.<br>• A ratio of 2047 sends copies of 1 out of every 2047 packets. | Enter a number from 0 through 2047. |
| Loss Priority<br><br>NOTE: This option is not supported on EX4300 switches. | Specifies the loss priority of the mirrored packets.<br><br>By default, the switch applies a lower priority to mirrored data than to regular port-to-port data—mirrored traffic is dropped in preference to regular traffic when capacity is exceeded.<br><br>For port-mirroring configurations with output to an analyzer VLAN, set the loss priority to high. | Keep the default of low, unless the output is to a VLAN. |
| Analyzer Port | Specifies a local interface or VLAN to which mirrored packets are sent.<br><br>NOTE: A VLAN must have only one associated interface to be specified as an analyzer interface. | Click **Select**. In the Select Analyzer Port/VLAN window, select either port or VLAN as the **Analyzer Type**. Next, select the required port or VLAN. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the port (interface) from the list. |
| Analyzer Type<br><br>NOTE: This option is supported only on EX4300 switches. | Specifies the analyzer type. | Select the **Analyzer Type** from the list. |
| No Filter check<br><br>NOTE: This option is supported only on EX4300 switches. | Enable this option to skip checking for filters on port-mirroring instance. | To enable this option, select the check box. |
| Ingress | Specifies interfaces or VLANs for which entering traffic is mirrored. | Click **Add**. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.<br><br>Click **Remove** to delete an ingress interface or VLAN. |
| Egress | Specifies interfaces for which exiting traffic is mirrored. | Click **Add** and select **Port** or **VLAN**. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.<br><br>Click **Remove** to remove egress interfaces. |

**Related Documentation**

- *Configuring Port Mirroring to Analyze Traffic (CLI Procedure)*


Copyright © 2016, Juniper Networks, Inc.

- *Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches*
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches*
- *Understanding Port Mirroring on EX Series Switches*

## Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches

**Purpose** Verify that an analyzer has been created on the switch and has the appropriate output interfaces, and appropriate output interface.

**Action** You can verify the port mirror analyzer is configured as expected 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, 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 sending the mirrored traffic to the analyzer called remote-analyzer.

Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- *Configuring Port Mirroring to Analyze Traffic (CLI Procedure)*
- *Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches*
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches*
- *Understanding Port Mirroring on EX Series Switches*

## 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 on page 54

### 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
   ```


Copyright © 2016, Juniper Networks, Inc.

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
   ```

**Related Documentation**

- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches*
- *Configuring Port Mirroring to Analyze Traffic (CLI Procedure)*
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 50
- *Understanding Port Mirroring on EX Series Switches*

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 3

# Configuring sFlow Monitoring Technology


- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 57
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64


## Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch

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 on page 57
- Adaptive Sampling on page 58
- sFlow Agent Address Assignment on page 59


### 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*.

Copyright © 2016, Juniper Networks, Inc.

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


Copyright © 2016, Juniper Networks, Inc.

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 on page 60

Copyright © 2016, Juniper Networks, Inc.

- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64
- *Monitoring Interface Status and Traffic*

## Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches

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 on page 60
- Overview and Topology on page 60
- Configuration on page 61
- Verification on page 63


### 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

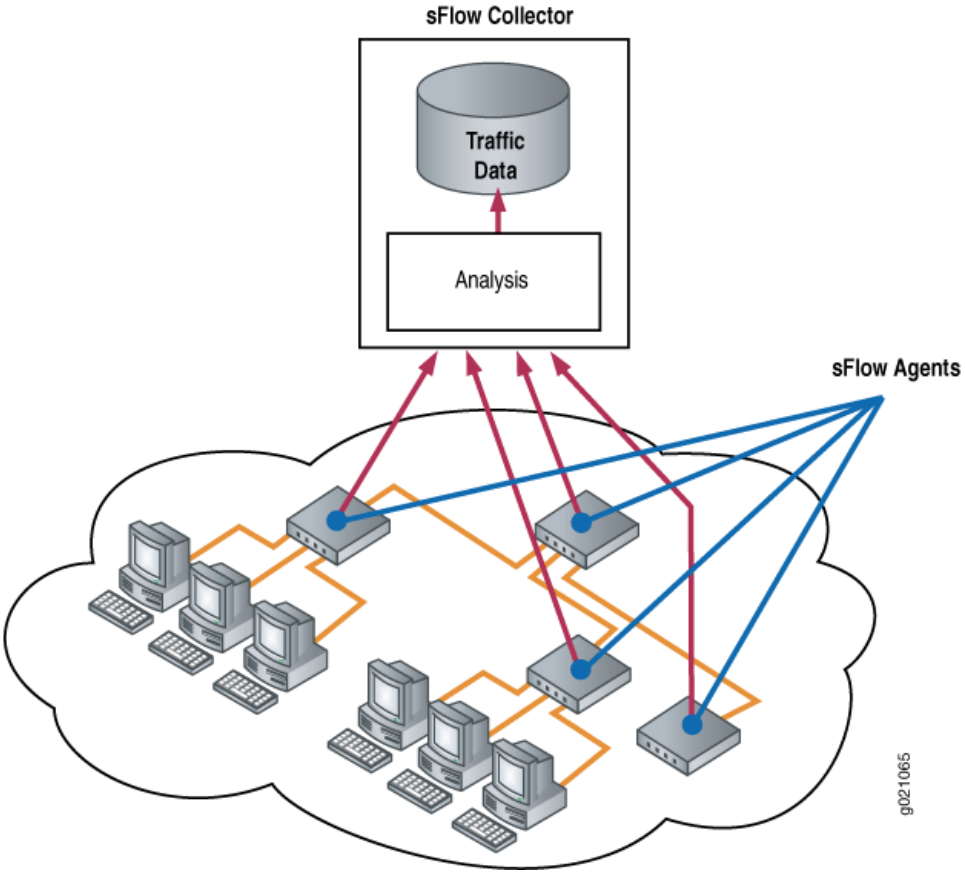
### Overview and Topology

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 5 on page 61 depicts the basic elements of the sFlow system.


Copyright © 2016, Juniper Networks, Inc.

Figure 5: 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
```

Copyright © 2016, Juniper Networks, Inc.

**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.


Copyright © 2016, Juniper Networks, Inc.

**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

To confirm that the configuration is correct, perform these tasks:

- Verifying That sFlow Technology Is Configured Properly on page 63
- Verifying That sFlow Technology Is Enabled on the Specified Interface on page 63
- Verifying the sFlow Collector Configuration on page 64

### 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
```

Copyright © 2016, Juniper Networks, Inc.

**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) on page 64
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 57

## 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*.

To configure sFlow features:

1. Configure the IP address and the UDP port of the collector:

   ```
   [edit protocols]
   user@switch# set sflow collector ip4/ipv6-address udp-port port-number
   ```

   The default UDP port is 6343,

2. Enable sFlow technology on a specific interface:

   ```
   [edit protocols sflow]
   user@switch# set interfaces interface-name
   ```

NOTE: 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.


Copyright © 2016, Juniper Networks, Inc.

3. Specify in seconds how often the sFlow agent polls interfaces:

```
[edit protocols sflow]
user@switch# 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@switch# set sample-rate egress number
```

To specify an ingress sampling rate:

```
[edit protocols sflow]
user@switch# set sample-rate ingress number
```

5. To configure the polling interval and the egress and ingress sampling rates at the interface level:

```
[edit protocols sflow interfaces interface-name]
user@switch# set polling-interval seconds
[edit protocols sflow interfaces]
user@switch# set sample-rate egress number
[edit protocols sflow interfaces]
user@switch# set sample-rate ingress number
```

NOTE: The interface-level configuration overrides the global configuration.

6. To specify an IP address to be used as the agent ID for the sFlow agent:

```
[edit protocols sflow]
user@switch# set agent-id ip4/ipv6 -address
```

7. To specify the source IP address to be used for sFlow datagrams:

```
[edit protocols sflow]
user@switch# set source-ip ip4/ipv6-address
```

**Related Documentation**

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 57

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 4

# Configuring Ethernet OAM Link Fault Management and Connectivity Fault Management


- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 67
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 69
- Understanding Ethernet Frame Delay Measurements on Switches on page 70
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 72
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 76
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83


## Understanding Ethernet OAM Link Fault Management for an EX Series Switch

Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet 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. 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.

Copyright © 2016, Juniper Networks, Inc.

- 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 on EX Series switches:

- 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 EX Series 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.

**Related Documentation**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 76


Copyright © 2016, Juniper Networks, Inc.

## Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch

Ethernet interfaces on Juniper Networks EX Series Ethernet Switches and Juniper Networks Junos operating system (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). 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 or link 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.

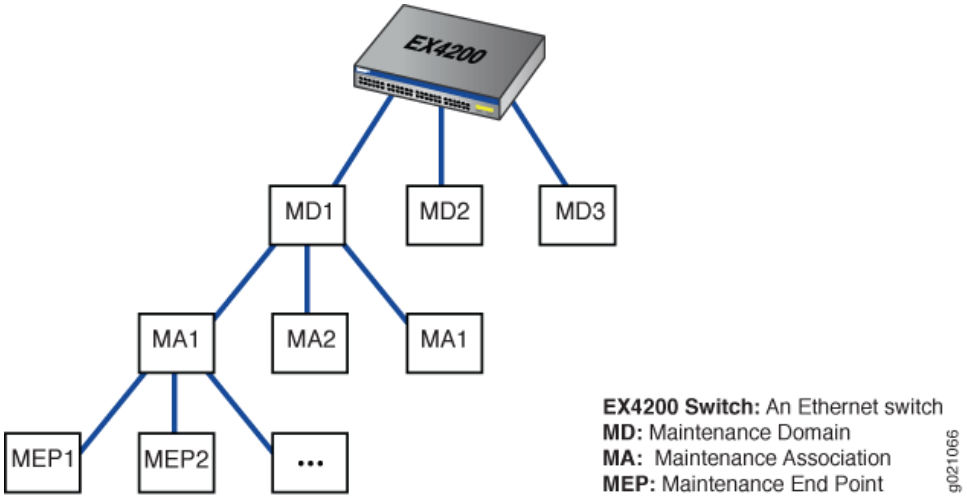
In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought of as a full mesh of maintenance association endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages. 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 6 on page 70 shows the relationships among maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs) configured on a switch.

Copyright © 2016, Juniper Networks, Inc. 

Figure 6: Relationship Among MEPs, MIPs, and Maintenance Domain Levels




**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79
- *Junos OS Network Interfaces Configuration Guide*

## Understanding Ethernet Frame Delay Measurements on Switches

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 on page 70
- Types of Ethernet Frame Delay Measurements on page 71
- Limitations on page 72

### 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)


Copyright © 2016, Juniper Networks, Inc.

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.

Copyright © 2016, Juniper Networks, Inc.

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)*
- *Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*
- *Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*
- *Triggering an Ethernet Frame Delay Measurement Session on a Switch*

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

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 on page 72
- Overview and Topology on page 73
- Configuring Ethernet OAM Connectivity Fault Management on Switch 1 on page 73
- Configuring Ethernet OAM Connectivity Fault Management on Switch 2 on page 74
- Verification on page 75


### 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


Copyright © 2016, Juniper Networks, Inc.

## 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;
              }
```

Copyright © 2016, Juniper Networks, Inc.

```
            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;
```


Copyright © 2016, Juniper Networks, Inc.

```
            maintenance-association private-ma {
              continuity-check {
                interval 1s;
              }
              mep 200 {
                interface ge-0/2/5;
                auto-discovery;
                direction down;
              }
            }
          }
        }
      }
```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That OAM CFM Has Been Configured Properly on page 75

### 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
```

Copyright © 2016, Juniper Networks, Inc.

**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 an EX Series Switch on page 69
- *Junos OS Network Interfaces Configuration Guide*

## Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches

Junos OS for EX Series 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 describes how to enable and configure OAM LFM on a Gigabit Ethernet interface:


- Requirements on page 76
- Overview and Topology on page 76
- Configuring Ethernet OAM Link Fault Management on Switch 1 on page 77
- Configuring Ethernet OAM Link Fault Management on Switch 2 on page 77
- Verification on page 78


### 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 for EX Series 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.


Copyright © 2016, Juniper Networks, Inc.

## 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 (OAM LFM) 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.


Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83
- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 67

## 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).

This topic describes these tasks:

1. Creating the Maintenance Domain on page 79
2. Configuring the Maintenance Domain MIP Half Function on page 80
3. Creating a Maintenance Association on page 80
4. Configuring the Continuity Check Protocol on page 80
5. Configuring a Maintenance Association End Point on page 81
6. Configuring a Connectivity Fault Management Action Profile on page 82
7. Configuring the Linktrace Protocol on page 82

### 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]
   ```

Copyright © 2016, Juniper Networks, Inc.

```
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

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
```


Copyright © 2016, Juniper Networks, Inc.

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).

   ```
   [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
   ```

Copyright © 2016, Juniper Networks, Inc.

## 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 on page 72
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 69
- *Junos OS Network Interfaces Configuration Guide*


Copyright © 2016, Juniper Networks, Inc.

## Configuring Ethernet OAM Link Fault Management (CLI Procedure)

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-name link-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-interval interval
   ```

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
     ```

Copyright © 2016, Juniper Networks, Inc.

- 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
```

**Related Documentation**

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 76
- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 67


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 5

# Configuring Uplink Failure Detection


- Understanding Uplink Failure Detection on page 85
- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 87
- Verifying That Uplink Failure Detection Is Working Correctly on page 88


## Understanding Uplink Failure Detection

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 on page 85
- Failure Detection Pair on page 86

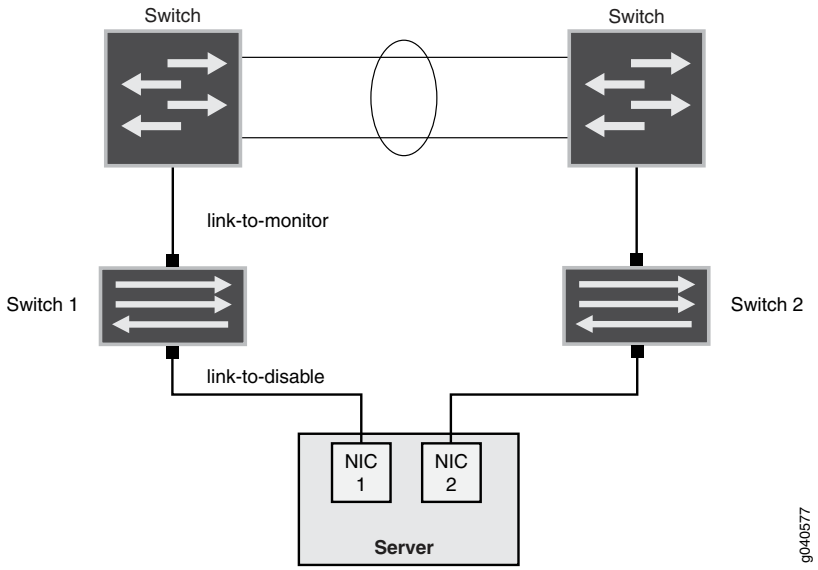

### Uplink Failure Detection Overview

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 7 on page 86 illustrates a typical setup for uplink failure detection.

Copyright © 2016, Juniper Networks, Inc.

Figure 7: 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.


Copyright © 2016, Juniper Networks, Inc.

- 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) on page 87

## 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.

Copyright © 2016, Juniper Networks, Inc.

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 on page 88
- Understanding Uplink Failure Detection on page 85

## 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) on page 87
- Understanding Uplink Failure Detection on page 85


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 6

# Configuring Network Analytics


- Network Analytics Overview on page 89
- Understanding Enhanced Network Analytics Streaming Data on page 97
- Understanding Enhanced Analytics Local File Output on page 102
- Prototype File for the Google Protocol Buffer Stream Format on page 104
- Example: Configuring Enhanced Network Analytics Features on page 105
- Configuring Queue Monitoring on page 115
- Configuring Traffic Monitoring on page 117
- Configuring a Local File for Network Analytics Data on page 118
- Configuring a Remote Collector for Streaming Analytics Data on page 119


## Network Analytics 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. 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.

Copyright © 2016, Juniper Networks, Inc.

For more information, see:


- Analytics Feature Overview on page 90
- Network Analytics Enhancements Overview on page 91
- Summary of CLI Changes on page 92


## 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.


Copyright © 2016, Juniper Networks, Inc.

## 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:

  http://www.juniper.net/techpubs/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.

Copyright © 2016, Juniper Networks, Inc.

- 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 8 on page 92 for a summary of CLI changes.

### Table 8: 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]**<br>traffic-statistics {<br>interval *interval*;<br>}<br>queue-statistics {<br>interval *interval*;<br>} | **[edit services analytics]**<br>resource {<br>system {<br>polling-interval {<br>queue-monitoring *interval*;<br>traffic-monitoring *interval*;<br>}<br>}<br>} |


Copyright © 2016, Juniper Networks, Inc.

Table 8: 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 local files for traffic and queue statistics reporting | **[edit services analytics]**<br>traffic-statistics {<br>file *filename*;<br>size *size*;<br>files *number*;<br>}<br>queue-statistics {<br>file *filename*;<br>size *size*;<br>files *number*;<br>} | **[edit services analytics]**<br>collector {<br>local {<br>file *filename* {<br>files *number*;<br>size *size*;<br>}<br>}<br>} |
| Enabling queue statistics and traffic monitoring, and specifying the depth threshold for all interfaces (globally) | **[edit services analytics]**<br>interfaces {<br>all {<br>queue-statistics;<br>traffic-statistics;<br>depth-threshold {<br>high *number*;<br>low *number*;<br>}<br>}<br>} | Requires defining a resource profile and applying it to the system:<br>1. To define a resource profile:<br>**[edit services analytics]**<br>resource-profiles {<br>*profile-name*{<br>queue-monitoring;<br>traffic-monitoring;<br>depth-threshold {<br>high *number*;<br>low *number*;<br>}<br>}<br>}<br>2. To apply a profile to the system:<br>**[edit services analytics]**<br>resource {<br>system {<br>resource-profile *profile-name*;<br>}<br>} |

Copyright © 2016, Juniper Networks, Inc.

Table 8: 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]**<br>interfaces {<br>*interface*{<br>queue-statistics;<br>traffic-statistics;<br>latency-threshold<br>high *number*;<br>low *number*;<br>}<br>} | Requires defining a resource profile and applying it to the interface:<br>1. To define a resource profile:<br>**[edit services analytics]**<br>resource-profiles {<br>*profile-name*{<br>queue-monitoring;<br>traffic-monitoring;<br>latency-threshold {<br>high *number*;<br>low *number*;<br>}<br>}<br>}<br>2. To apply a profile to the interface:<br>**[edit services analytics]**<br>resource {<br>interfaces {<br>*interface-name* {<br>resource-profile *profile-name*;<br>}<br>}<br>} |
| Configuring the streaming data format (JSON, CSV, or TSV) to send to a remote server<br>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]**<br>streaming-servers {<br>address *ip-address* {<br>port *number* {<br>stream-format *format*;<br>}<br>}<br>} | Requires defining the stream format in an export profile and applying the profile to the collector.<br>1. To configure the stream format:<br>**[edit services analytics]**<br>export-profiles {<br>*profile-name* {<br>stream-format *format*;<br>}<br>}<br>2. To apply an export profile to the collector:<br>**[edit services analytics]**<br>collector {<br>address *ip-address* {<br>port *number* {<br>transport *protocol* {<br>export-profile *profile-name*;<br>}<br>}<br>}<br>} |


Copyright © 2016, Juniper Networks, Inc.

Table 8: 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]**<br>streaming-servers {<br>address *ip-address* {<br>port *number* {<br>stream-type *type*;<br>stream-type *type*;<br>}<br>}<br>} | Requires defining an export profile and applying it to the collector:<br>1. To define an export profile:<br>**[edit services analytics]**<br>export-profiles {<br>*profile-name* {<br>interface {<br>information;<br>statistics {<br>queue;<br>traffic;<br>}<br>status {<br>link;<br>queue;<br>traffic;<br>}<br>}<br>system {<br>information;<br>status {<br>queue;<br>traffic;<br>}<br>}<br>}<br>}<br>2. To apply an export profile to the collector:<br>**[edit services analytics]**<br>collector {<br>address *ip-address* {<br>port *number* {<br>export-profile *profile-name*;<br>}<br>}<br>} |

Copyright © 2016, Juniper Networks, Inc.

Table 8: 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.<br>**[edit services analytics]**<br>collector {<br>address *ip-address* {<br>port *number1* {<br>transport tcp;<br>transport udp;<br>}<br>port *number2* {<br>transport udp;<br>}<br>}<br>} |
| 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. |

**Related Documentation**

- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## Understanding Enhanced Network Analytics Streaming Data

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) on page 97
- JavaScript Object Notation (JSON) on page 99
- Comma-separated Values (CSV) on page 100
- Tab-separated Values (TSV) on page 100
- Queue Statistics Output for JSON, CSV, and TSV on page 100
- Traffic Statistics Output for JSON, CSV, and TSV on page 101


### 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 9 on page 97 for more information.

Table 9 on page 97 describes the GPB stream format message header.

**Table 9: 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 |

Copyright © 2016, Juniper Networks, Inc.

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;
```


Copyright © 2016, Juniper Networks, Inc.

```
    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:

Copyright © 2016, Juniper Networks, Inc.

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

See Table 10 on page 101 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 11 on page 101 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 10 on page 101 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 11 on page 101 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 10 on page 101 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 11 on page 101 for more information about traffic statistics output fields.

## Queue Statistics Output for JSON, CSV, and TSV

Table 10 on page 101 describes the output fields for streamed queue statistics data in the order they appear.


Copyright © 2016, Juniper Networks, Inc.

### Table 10: Streamed Queue Statistics Data Output Fields

| Field | Description |
|---|---|
| record-type | Type of statistics. Displayed as:<br>• **queue-stats** (JSON format)<br>• **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 11 on page 101 describes the output fields for streamed traffic statistics data in the order they appear.

### Table 11: Streamed Traffic Statistics Data Output Fields

| Field | Description |
|---|---|
| record-type | Type of statistics. Displayed as:<br>• **traffic-stats** (JSON format)<br>• **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. |

Copyright © 2016, Juniper Networks, Inc.

Table 11: Streamed Traffic Statistics Data Output Fields *(continued)*

| Field | Description |
|---|---|
| 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 on page 89
- Prototype File for the Google Protocol Buffer Stream Format on page 104
- **address (Analytics Collector) on page 224**
- **collector (Analytics) on page 229**
- *show analytics collector*

## 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. For information about local file output from earlier releases, see the *monitor start (Analytics)* topic.**

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
```


Copyright © 2016, Juniper Networks, Inc.

```
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 12 on page 103 for queue statistics output, and Table 13 on page 103 for traffic statistics output. The fields in the tables are listed in the order they appear in the output example.

### Table 12: 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 13: 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** |

Copyright © 2016, Juniper Networks, Inc.

Table 13: Output Fields for Traffic Statistics in Local Analytics File *(continued)*

| Field | Description | Example in Output |
|---|---|---|
| rxpps | Total packets received per second. | **8426023** |
| rxbyte | Total octets received. | **1613231610488** |
| rxbps | Total bytes received per second. | **8628248712** |
| 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 on page 89
- analytics on page 225

## 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.


Copyright © 2016, Juniper Networks, Inc.

To download the GPB prototype file, go to:

http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt

**Related Documentation**

- Network Analytics Overview on page 89
- **analytics on page 225**
- **export-profiles on page 231**

## Example: Configuring Enhanced Network Analytics Features

This example shows how to configure the enhanced network analytics feature, including queue and traffic monitoring.


- Requirements on page 105
- Overview on page 105
- Configuration on page 106
- Verification on page 111


### 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.

Copyright © 2016, Juniper Networks, Inc.

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

To configure the network analytics features, perform these tasks:

- Configuring the Polling Interval for Queue and Traffic Monitoring on page 107
- Configuring a Local Statistics File on page 107
- Configuring and Applying a Resource Profile for the System on page 107
- Configuring and Applying a Resource Profile for an Interface on page 108
- Configuring an Export Profile and Collector for Streaming Data on page 108

**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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
   ```

Copyright © 2016, Juniper Networks, Inc.

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:


Copyright © 2016, Juniper Networks, Inc.

```
[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 {
```

Copyright © 2016, Juniper Networks, Inc.

```
            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 {
```


Copyright © 2016, Juniper Networks, Inc.

```
            transport udp {
              export-profile ep;
            }
          }
        }
        address 10.94.198.11 {
          port 50001 {
            transport tcp {
              export-profile ep;
            }
          }
        }
      }
    }
  }
```

## Verification

Confirm that the configuration is correct and works as expected by performing these tasks:


- Verifying the Network Analytics Configuration on page 111
- Verifying the Network Analytics Status on page 112
- Verifying the Collector Configuration on page 112
- Verifying Queue Statistics on page 113
- Verifying Traffic Statistics on page 113


### 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.


Copyright © 2016, Juniper Networks, Inc.

### 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.

Copyright © 2016, Juniper Networks, Inc.

**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 on page 89
- analytics on page 225
- *show analytics status*
- *show analytics collector*


Copyright © 2016, Juniper Networks, Inc.

## 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***

Copyright © 2016, Juniper Networks, Inc.

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 on page 89
- Example: Configuring Enhanced Network Analytics Features on page 105
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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***

Copyright © 2016, Juniper Networks, Inc.

**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 on page 89
- Example: Configuring Enhanced Network Analytics Features on page 105
- **analytics on page 225**

## 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 *x*m:

   [edit]
   **set services analytics collector local file an size *size***


Copyright © 2016, Juniper Networks, Inc.

**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 on page 89
- Example: Configuring Enhanced Network Analytics Features on page 105
- **analytics on page 225**

## 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**

Copyright © 2016, Juniper Networks, Inc.

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 on page 89
- Example: Configuring Enhanced Network Analytics Features on page 105
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 7

# Configuring SNMP


- Configuring SNMP (J-Web Procedure) on page 121
- Configuring the Local Engine ID on page 124


## Configuring SNMP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define system identification information, create SNMP communities, create SNMP trap groups, and configure health monitor options for EX Series switches.

To configure SNMP features:

1. Select **Configure** > **Services** > **SNMP**.
2. Enter information into the configuration page for SNMP as described in Table 14 on page 121.
3. To apply the configuration click **Apply**.

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

### Table 14: SNMP Configuration Page

| Field | Function | Your Action |
|---|---|---|
| Identification | | |
| Contact Information | Free-form text string that specifies an administrative contact for the system. | Type contact information for the administrator of the system (such as name and phone number). |

Copyright © 2016, Juniper Networks, Inc.

Table 14: SNMP Configuration Page *(continued)*

| Field | Function | Your Action |
|---|---|---|
| System Description | Free-form text string that specifies a description for the system. | Type information that describes the system |
| Local Engine ID | Provides an administratively unique identifier of an SNMPv3 engine for system identification.<br><br>The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0. | Type the MAC address of Ethernet management port 0. |
| System Location | Free-form text string that specifies the location of the system. | Type location information for the system (lab name or rack name, for example). |
| System Override Name | Free-form text string that overrides the system hostname. | Type the hostname of the system. |
| **Communities**<br><br>To add a community, click **Add** | | |
| Community Name | Specifies the name of the SNMP community. | Type the name of the community being added. |
| Authorization | Specifies the type of authorization (either read-only or read-write) for the SNMP community being configured. | Select the authorization (either read-only or read-write) from the list. |
| **Traps**<br><br>To add a trap group, click **Add**. | | |
| Trap Group Name | Specifies the name of the SNMP trap group being configured. | Type the name of the group being added. |


Copyright © 2016, Juniper Networks, Inc.

Table 14: SNMP Configuration Page *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Categories | Specifies which trap categories are added to the trap group being configured. | • To generate traps for authentication failures, select **Authentication**.<br>• To generate traps for chassis and environment notifications, select **Chassis**.<br>• To generate traps for configuration changes, select **Configuration**.<br>• To generate traps for link-related notifications (up-down transitions), select **Link**.<br>• To generate traps for remote operation notifications, select **Remote operations**.<br>• To generate traps for remote network monitoring (RMON), select **RMON alarm**.<br>• To generate traps for routing protocol notifications, select **Routing**.<br>• To generate traps on system warm and cold starts, select **Startup**.<br>• To generate traps on Virtual Router Redundancy Protocol (VRRP) events (such as new-master or authentication failures), select **VRRP events**. |
| Targets | Specifies one or more hostnames or IP addresses for the systems to receive SNMP traps generated by the trap group being configured. | 1. Enter the hostname or IP address, in dotted decimal notation, of the target system to receive the SNMP traps.<br>2. Click **Add**. |
| Health Monitoring | | |
| Enable Health Monitoring | Enables the SNMP health monitor on the switch. The health monitor periodically (over the time you specify in the interval field) checks the following key indicators of switch health:<br>• Percentage of file storage used<br>• Percentage of Routing Engine CPU used<br>• Percentage of Routing Engine memory used<br>• Percentage of memory used for each system process<br>• Percentage of CPU used by the forwarding process<br>• Percentage of memory used for temporary storage by the forwarding process | Select the check box to enable the health monitor and configure options. Clear the check box to disable the health monitor.<br>NOTE: If you select the **Enable Health Monitoring** check box and do not specify options, then SNMP health monitoring is enabled with default values. |
| Interval | Specifies the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds.<br>For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds. | Enter an interval time, in seconds, from **1** through **2147483647**.<br>The default value is 300 seconds (5 minutes). |

Copyright © 2016, Juniper Networks, Inc.

Table 14: SNMP Configuration Page *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Rising Threshold | Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is increasing.<br><br>For example, if the rising threshold is 90 (the default), SNMP generates an event when the value of any key indicator reaches or exceeds 90 percent. | Enter a value from **0** through **100**. The default value is **90**. |
| Falling Threshold | Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is decreasing.<br><br>For example, if the falling threshold is 80 (the default), SNMP generates an event when the value of any key indicator falls back to 80 percent or less. | Enter a value from **0** through **100**. The default value is **80**.<br><br>NOTE: The falling threshold value must be less than the rising threshold value. |

**Related Documentation**

- *Monitoring System Process Information*
- *Monitoring System Properties*

## 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.

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.


Copyright © 2016, Juniper Networks, Inc.

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*
- *Example: SNMPv3 Configuration*

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 8

# Monitoring and Troubleshooting


- Monitoring Hosts Using the J-Web Ping Host Tool on page 127
- Monitoring Network Traffic Using Traceroute on page 129


## Monitoring Hosts Using the J-Web Ping Host Tool

**Purpose**

NOTE: This topic applies only to the J-Web Application package.

Use the J-Web ping host tool to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The switch sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

**Action** To use the J-Web ping host tool:

1. Select **Troubleshoot>Ping Host**.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page, as described in Table 15 on page 127.

   The Remote Host field is the only required field.
4. Click **Start**.

   The results of the ping operation are displayed in the main pane . If no options are specified, each ping response is in the following format:

   ```
   bytes bytes from ip-address: icmp_seq=number ttl=number time=time
   ```
5. To stop the ping operation before it is complete, click **OK**.

**Meaning** Table 15 on page 127 lists the fields.

### Table 15: J-Web Ping Host Field Summary

| Field | Function | Your Action |
|---|---|---|
| Remote Host | Identifies the host to ping. | Type the hostname or IP address of the host to ping. |
| Advanced Options | | |

Copyright © 2016, Juniper Networks, Inc.

Table 15: J-Web Ping Host Field Summary *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Don't Resolve Addresses | Determines whether to display hostnames of the hops along the path. | • To suppress the display of the hop hostnames, select the check box.<br>• To display the hop hostnames, clear the check box. |
| Interface | Specifies the interface on which the ping requests are sent. | Select the interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces. |
| Count | Specifies the number of ping requests to send. | Select the number of ping requests to send from the list. |
| Don't Fragment | Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet. | • To set the DF bit, select the check box.<br>• To clear the DF bit, clear the check box. |
| Record Route | 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 in the main pane. | • To record and display the path of the packet, select the check box.<br>• To suppress the recording and display of the path of the packet, clear the check box. |
| Type-of-Service | Specifies the type-of-service (TOS) value in the IP header of the ping request packet. | Select the decimal value of the TOS field from the list. |
| Routing Instance | Name of the routing instance for the ping attempt. | Select the routing instance name from the list. |
| Interval | Specifies the interval, in seconds, between transmissions of individual ping requests. | Select the interval from the list. |
| Packet Size | Specifies the size of the ping request packet. | Type the size, in bytes, of the packet. The size can be from 0 through 65468. The switch adds 8 bytes of ICMP header to the size. |
| Source Address | Specifies the source address of the ping request packet. | Type the source IP address. |
| Time-to-Live | Specifies the time-to-live (TTL) hop count for the ping request packet. | Select the TTL value from the list. |
| Bypass Routing | Determines whether ping requests are routed by means of the routing table.<br>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent. | • To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box.<br>• To route the ping requests using the routing table, clear the check box. |

**Related Documentation**

- *Monitoring Interface Status and Traffic*


Copyright © 2016, Juniper Networks, Inc.

## Monitoring Network Traffic Using Traceroute

**Purpose**

NOTE: This topic applies only to the J-Web Application package.

Use the Traceroute page in the J-Web interface to trace a route between the switch and a remote host. You can use a traceroute task to display a list of waypoints between the switch and a specified destination host. The output is useful for diagnosing a point of failure in the path from the switch platform to the destination host and addressing network traffic latency and throughput problems.

**Action**

To use the traceroute tool:

1. Select **Troubleshoot** > **Traceroute**.
2. Next to **Advanced options**, click the expand icon.
3. Enter information into the Traceroute page.

   The **Remote Host** field is the only required field.
4. Click **Start**.
5. To stop the traceroute operation before it is complete, click **OK** while the results of the traceroute operation are being displayed.

**Meaning**

The switch generates the list of waypoints by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive waypoint is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each waypoint along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

**hop-number host (ip-address) [as-number] time1 time2 time3**

The switch sends a total of three traceroute packets to each waypoint along the path and displays the round-trip time for each traceroute operation. If the switch times out before receiving a **Time Exceeded** message, an asterisk (*) is displayed for that round-trip time.

### Table 16: Traceroute field summary

| Field | Function | Your Action |
|---|---|---|
| Remote Host | Identifies the destination host of the traceroute. | Type the hostname or IP address of the destination host. |
| Advanced Options | | |

Copyright © 2016, Juniper Networks, Inc.

Table 16: Traceroute field summary *(continued)*

| Field | Function | Your Action |
|---|---|---|
| Don't Resolve Addresses | Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses. | To suppress the display of the hop hostnames, select the check box. |
| Gateway | Specifies the IP address of the gateway to route through. | Type the gateway IP address. |
| Source Address | Specifies the source address of the outgoing traceroute packets. | Type the source IP address. |
| Bypass Routing | Determines whether traceroute packets are routed by means of the routing table. If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent. | To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box. |
| Interface | Specifies the interface on which the traceroute packets are sent. | From the list, select the interface on which traceroute packets are sent. If you select any, the traceroute requests are sent on all interfaces. |
| Time-to-live | Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet. | From the list, select the TTL. |
| Type-of-Service | Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet. | From the list, select the decimal value of the TOS field. |
| Resolve AS Numbers | Determines whether the autonomous system (AS) number of each intermediate hop between the router and the destination host is displayed. | To display the AS numbers, select the check box. |

**Related Documentation**

- *Connecting and Configuring an EX Series Switch (CLI Procedure)*
- *Connecting and Configuring an EX Series Switch (J-Web Procedure)*
- *Configuring Gigabit Ethernet Interfaces (J-Web Procedure)*
- *Monitoring Interface Status and Traffic*


Copyright © 2016, Juniper Networks, Inc.

PART 2

# Configuration Statements


- Realtime Performance Monitoring on page 133
- Analyzers and Port Mirroring on page 159
- sFlow Monitoring Technology on page 167
- Ethernet OAM Link Fault Management and Connectivity Fault Management on page 175
- Uplink Failure Detection on page 217
- Network Analytics on page 223
- SNMP on page 245


Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 9

# Realtime Performance Monitoring


- data-fill on page 134
- data-size on page 135
- destination-port on page 136
- dscp-code-point on page 137
- hardware-timestamp on page 138
- history-size on page 139
- moving-average-size on page 140
- one-way-hardware-timestamp on page 140
- port (RPM) on page 141
- probe on page 142
- probe-count on page 143
- probe-interval on page 144
- probe-limit on page 145
- probe-server on page 146
- probe-type on page 147
- routing-instance on page 148
- routing-instances on page 149
- rpm (Interfaces) on page 150
- source-address (Services) on page 151
- tcp on page 152
- test on page 153
- test-interval on page 154
- thresholds on page 155
- traps on page 157
- udp on page 158


Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*):

- 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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

Copyright © 2016, Juniper Networks, Inc.

- **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*
- *Two-Way Active Measurement Protocol Overview*

## 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.

**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.


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*

## 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.

**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.

**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*
- *destination-interface*
- hardware-timestamp on page 138

 Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## probe

**Syntax**

```
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;
    inet6-options source-address ipv6-address;
    moving-average-size number;
    next-hop next-hop;
    one-way-hardware-timestamp;
    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance instance-name;
    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];
  }
}
```

**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.

**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.

 Copyright © 2016, Juniper Networks, Inc.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*
- *Two-Way Active Measurement Protocol Overview*


Copyright © 2016, Juniper Networks, Inc.

## 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.

**Description** Configure the maximum number of concurrent probes allowed.

**Options** ***limit***—Maximum number of concurrent probes allowed.

**Range:** (PTX Series Packet Transport routers only) 1 through 200
(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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**Description** Specify the server to act as a receiver for the probes.

The remaining statements are explained separately.

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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Two-Way Active Measurement Protocol Overview*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**Description** Specify the port information for the TCP server.

The remaining statements are explained separately.

**Required Privilege Level**

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

**Related Documentation**

- *Configuring RPM Receiver Servers*


Copyright © 2016, Juniper Networks, Inc.

## 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;
  source-address address;
  target (url url | address address);
  test-interval interval;
  thresholds thresholds;
  traps traps;
}
```

**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.

**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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Two-Way Active Measurement Protocol Overview*


Copyright © 2016, Juniper Networks, Inc.

## thresholds

**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.

Copyright © 2016, Juniper Networks, Inc.

**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*
- *Two-Way Active Measurement Protocol Overview*


Copyright © 2016, Juniper Networks, Inc.

## 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.

Copyright © 2016, Juniper Networks, Inc.

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*
- *Two-Way Active Measurement Protocol Overview*

## 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.

**Description**
Specify the port information for the UDP server.

The remaining statements are explained separately.

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*


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 10

# Analyzers and Port Mirroring


- egress on page 159
- egress (Analyzer) on page 160
- ingress (vlans) on page 160
- ingress (Analyzer) on page 161
- input (Analyzer) on page 162
- interface (Analyzer) on page 163
- no-tag on page 164
- output (Mirroring) on page 165
- vlan (Mirroring) on page 166


## egress

**Syntax** egress;

**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 egress traffic.

**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 Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*

## 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.

**Related Documentation**

- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches*


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

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.


Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- *Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use*
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use*
- *Understanding Port Mirroring Analyzers*

## 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*
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use*
- *Understanding Port Mirroring Analyzers*

Copyright © 2016, Juniper Networks, Inc.

## 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 Local Monitoring of Employee Resource Use on EX4300 Switches on page 23
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 30


Copyright © 2016, Juniper Networks, Inc.

## 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.

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

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use*


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 11

# sFlow Monitoring Technology


- agent-id on page 167
- collector on page 168
- disable (sFlow Monitoring Technology) on page 168
- interfaces (sFlow Monitoring Technology) on page 169
- polling-interval on page 170
- sample-rate on page 171
- sflow on page 172
- source-ip on page 173
- udp-port on page 173


## agent-id

**Syntax** agent-id *ip4/ipv6-address*;

**Hierarchy Level** [edit protocols sflow]

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

**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.

**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) on page 64

Copyright © 2016, Juniper Networks, Inc.

## collector

**Syntax**

```
collector {
  ip4/ipv6-address;
  udp-port port-number;
}
```

**Hierarchy Level** [edit protocols sflow]

**Release Information** Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description** Configure a remote collector for sFlow network traffic monitoring. The switch sends sFlow UDP datagrams to this collector for analysis. You can configure up to four collectors on the switch. You configure a collector by specifying its IP address and a UDP port.

The remaining statements are explained separately.

**Default** The default port is 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 on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

## 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.

**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 on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64


Copyright © 2016, Juniper Networks, Inc.

## interfaces (sFlow Monitoring Technology)

**Syntax**

```
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.

**Description** Configure sFlow network traffic monitoring on the specified interface on the switch. 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.

**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**

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

Copyright © 2016, Juniper Networks, Inc.

## 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.

**Description** Configure the interval (in seconds) that the switch waits between port statistics update messages. *Polling* refers to the switch 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 switch waits the number of seconds that is configured as the polling interval in the global sFlow configuration. If no polling interval is specified in the global configuration, the switch waits 20 seconds between messages.

**Options** *seconds*—Number of seconds between port statistics update messages. A value of **0** (zero) specifies that polling is disabled.

**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) on page 64
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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:** 100 through 1,073,741,823

**ingress *number***—Value for ingress sampling rate.

**Range:** 100 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) on page 64
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60

Copyright © 2016, Juniper Networks, Inc.

## sflow

**Syntax**

```
sflow {
  agent-id ip-address;
  collector {
    ip-address;
    udp-port port-number;
  }
  interfaces interface-name {
    disable;
    polling-interval seconds;
    sample-rate {
    egress number;
    ingress number;
    }
  }
  polling-interval seconds;
  sample-rate {
  egress number;
  ingress number;
  }
  source-ip ip-address;
}
```

**Hierarchy Level** [edit protocols]

**Release Information** Statement introduced in Junos OS Release 9.3 for EX Series switches.
Options **agent-id** and **source-ip** added in Junos OS Release 10.2 for EX Series switches.

**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.

The remaining statements are explained separately.

**Default** sFlow technology is disabled by default.

**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 on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64


Copyright © 2016, Juniper Networks, Inc.

## source-ip

**Syntax** source-ip *ip4/ipv6-address*;

**Hierarchy Level** [edit protocols sflow]

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

**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.

**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) on page 64

## 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.

**Description** Configure the UDP port for a remote collector for sFlow network traffic monitoring. The switch 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 on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 12

# Ethernet OAM Link Fault Management and Connectivity Fault Management


- action-profile (Applying to OAM CFM, for EX Series Switch Only) on page 177
- age (EX Series Switch Only) on page 178
- auto-discovery (EX Series Switch Only) on page 178
- calculation-weight on page 179
- connectivity-fault-management (EX Series Switch Only) on page 180
- continuity-check (EX Series Switch Only) on page 181
- cycle-time on page 182
- delay on page 183
- delay-variation on page 184
- direction (EX Series Switch Only) on page 185
- hold-interval (OAM CFM, for EX Series Switch Only) on page 185
- interface (OAM CFM, for EX Series Switch Only) on page 186
- interval (EX Series Switch Only) on page 187
- iteration-period on page 188
- level (EX Series Switch Only) on page 188
- linktrace (EX Series Switch Only) on page 189
- loss-threshold (EX Series Switch Only) on page 189
- maintenance-association (EX Series Switch Only) on page 190
- maintenance-domain (EX Series Switch Only) on page 191
- measurement-type (OAM LFM) on page 192
- mep (EX Series Switch Only) on page 193
- mip-half-function (EX Series Switch Only) on page 194
- name-format (EX Series Switch Only) on page 195
- path-database-size (EX Series Switch Only) on page 195
- performance-monitoring (OAM LFM) on page 196
- remote-mep (EX Series Switch Only) on page 197


Copyright © 2016, Juniper Networks, Inc.

- sla-iterator-profiles (OAM LFM) on page 198
- action (OAM LFM) on page 198
- action-profile on page 199
- allow-remote-loopback on page 200
- ethernet (OAM LFM) on page 201
- event (OAM LFM) on page 204
- event-thresholds on page 204
- frame-error on page 205
- frame-period on page 205
- frame-period-summary on page 206
- interface (OAM LFM) on page 207
- link-adjacency-loss on page 208
- link-discovery on page 208
- link-down on page 209
- link-event-rate on page 209
- link-fault-management on page 210
- negotiation-options on page 211
- no-allow-link-events on page 211
- oam on page 212
- pdu-interval on page 214
- pdu-threshold on page 215
- remote-loopback on page 215
- symbol-period on page 216
- syslog (OAM LFM) on page 216



Copyright © 2016, Juniper Networks, Inc.

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## age (EX Series Switch Only)

**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 10.2 for EX Series switches.

**Description** Configure the 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** 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*


Copyright © 2016, Juniper Networks, Inc.

## 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.

**Required Privilege Level**

Configure—To enter configuration mode.
Control—To modify any configuration.

**Related Documentation**

- *Configuring an Iterator Profile*
- *Configuring an Iterator Profile on a Switch (CLI Procedure)*
- delay on page 183
- delay-variation on page 184

Copyright © 2016, Juniper Networks, Inc.

## 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;
      }
    }
  }
```


Copyright © 2016, Juniper Networks, Inc.

```
}
```

**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.

**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) on page 79
- *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.

**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.

**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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring an Iterator Profile on a Switch (CLI Procedure)*


Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring an Iterator Profile on a Switch (CLI Procedure)*
- calculation-weight on page 179

Copyright © 2016, Juniper Networks, Inc. 

## 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*
- *Configuring an Iterator Profile on a Switch (CLI Procedure)*
- calculation-weight on page 179


Copyright © 2016, Juniper Networks, Inc.

## direction (EX Series Switch Only)

**Syntax** direction 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 10.2 for EX Series switches.

**Description** Specify that connectivity fault management (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.

**Options** **down**—Down MEP CCMs are transmitted only out (not into) of the interface configured on this 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

 Copyright © 2016, Juniper Networks, Inc.

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring an Iterator Profile on a Switch (CLI Procedure)*

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*


Copyright © 2016, Juniper Networks, Inc.

## linktrace (EX Series Switch Only)

**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 10.2 for EX Series switches.

**Description** Configure connectivity fault management linktrace parameters.

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**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79
- *Junos OS Network Interfaces Configuration Guide*

## loss-threshold (EX Series Switch Only)

**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 10.2 for EX Series switches.

**Description** Configure the number of continuity check messages that can be lost before the remote MEP is marked as down.

**Options** *number*—Number of continuity check messages that can be lost before the remote MEP is marked down.

**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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## maintenance-association (EX Series Switch Only)

**Syntax**

```
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;
    }
  }
}
```

**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 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.

**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) on page 79
- *Junos OS Network Interfaces Configuration Guide*


Copyright © 2016, Juniper Networks, Inc.

## maintenance-domain (EX Series Switch Only)

**Syntax**

```
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;
      }
    }
  }
}
```

**Hierarchy Level** [edit protocols oam ethernet connectivity-fault-management ]

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

**Description** Configure the name of the maintenance domain in IEEE-compliant format.

**Options** *domain-name*—The name for the maintenance domain.

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**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## measurement-type (OAM LFM)

**Syntax** measurement-type 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 11.4 for EX Series switches.

**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** **two-way-delay**—Use Y.1731-compliant two-way ETH-DM frames to measure frame loss.

**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)*
- *Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*
- *Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*


Copyright © 2016, Juniper Networks, Inc.

## mep (EX Series Switch Only)

**Syntax**

```
mep mep-id {
  auto-discovery;
  direction down;
  interface interface-name;
  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*]

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

**Description** Configure the numeric identifier of the 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.

**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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## mip-half-function (EX Series Switch Only)

**Syntax** mip-half-function (none | default | explicit);

**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** Specify the OAM Ethernet CFM maintenance domain MIP half functions.

NOTE: Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be 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**

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) on page 79
- *Junos OS Network Interfaces Configuration Guide*


Copyright © 2016, Juniper Networks, Inc.

## name-format (EX Series Switch Only)

**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 10.2 for EX Series switches.

**Description** Specify the format of the maintenance domain name.

**Options**

**character-string**—The name is an ASCII character string.

**none**—Name format **none** means that maintenance domain name is not used.

**dns**—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** 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

## 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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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)*
- *Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*
- *Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)*


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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) on page 79
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## sla-iterator-profiles (OAM LFM)

**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.

**Required Privilege Level** Configure—To enter configuration mode.
Control—To modify any configuration.

**Related Documentation**

- *Configuring an Iterator Profile on a Switch (CLI Procedure)*

## 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.

**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 (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## action-profile

**Syntax**

```
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 9.4 for EX Series switches.

**Description** Configure an Ethernet OAM link fault management (LFM) action profile by specifying a profile name.

The remaining statements are explained separately.

**Options** *profile-name*—Name of the action profile.

**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 (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## ethernet (OAM LFM)

**Syntax**

```
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-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;
          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 {
```

Copyright © 2016, Juniper Networks, Inc.

```
    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;
```


Copyright © 2016, Juniper Networks, Inc.

```
    }
  }
}
```

**Hierarchy Level** [edit protocols oam]

**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) 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.

**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 on EX Series Switches on page 76
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 72
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79

Copyright © 2016, Juniper Networks, Inc.

## event (OAM LFM)

**Syntax**

```
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 *profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description** Configure link events in an action profile for Ethernet OAM link fault management (LFM).

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**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83

## 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.

**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 (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## 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 (CLI Procedure) on page 83

## 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 (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## 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 (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## interface (OAM LFM)

**Syntax**

```
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 link-fault-management]

**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.

**Options** *interface-name*—Name of the interface to be enabled for IEEE 802.3ah 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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## 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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83

## 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 (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## 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 (CLI Procedure) on page 83

## 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.

**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 (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 (CLI Procedure) on page 83

## 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 (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## 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;
          }
```


Copyright © 2016, Juniper Networks, Inc.

```
        }
      }
    }
    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.

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

Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 76
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 72
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 79

## 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 9.4 for EX Series switches.

**Description** Specify the periodic OAM PDU sending interval for fault detection. It is used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support.

**Options** *interval*—Periodic OAM PDU sending interval.

**Range:** 400 through 1000 milliseconds

**Default:** 1000 milliseconds

**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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

## 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 9.4 for EX Series switches.

**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.

**Options** ***threshold-value*** —Number of PDUs missed before declaring the peer lost.

**Range:** 3 through 10 PDUs

**Default:** 3 PDUs

**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 (CLI Procedure) on page 83

## 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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83

Copyright © 2016, Juniper Networks, Inc.

## symbol-period

**Syntax** symbol-period *count*;

**Hierarchy Level** [edit protocols oam ethernet link-fault-management action-profile *profile-name*; 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 (CLI Procedure) on page 83

## syslog (OAM LFM)

**Syntax** syslog;

**Hierarchy Level** [edit protocols oam ethernet link-fault-management action-profile *profile-name*; action]

**Release Information** Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description** Generate a system log message for the Ethernet Operation, Administration, and Maintenance (OAM) link fault management (LFM) event.

**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 (CLI Procedure) on page 83


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 13

# Uplink Failure Detection


- action (Uplink Failure Detection) on page 217
- group (Uplink Failure Detection) on page 218
- link-to-disable on page 218
- link-to-monitor on page 219
- traceoptions (Uplink Failure Detection) on page 220
- uplink-failure-detection on page 221


## 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) on page 87

Copyright © 2016, Juniper Networks, Inc.

## group (Uplink Failure Detection)

**Syntax**

```
group group-name {
  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.

**Options** *group-name*—Name of the uplink-failure-detection group.

The remaining statements are explained separately.

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

**Related Documentation**

- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 87

## 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) on page 87


Copyright © 2016, Juniper Networks, Inc.

## 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) on page 87

Copyright © 2016, Juniper Networks, Inc.

## 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 ( ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** 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


Copyright © 2016, Juniper Networks, Inc.

**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) on page 87

## uplink-failure-detection

**Syntax**

```
uplink-failure-detection {
  action {
    log;
  }
  group group-name {
    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.

**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.

**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) on page 87

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 14

# Network Analytics


- address (Analytics Collector) on page 224
- analytics on page 225
- collector (Analytics) on page 229
- depth-threshold on page 230
- export-profiles on page 231
- file (Analytics) on page 233
- interface (Export Profiles) on page 235
- interfaces (Analytics Resource) on page 236
- latency-threshold on page 237
- local (Analytics Collector) on page 238
- resource (Analytics) on page 239
- resource-profiles (Analytics) on page 240
- system (Analytics Resource) on page 241
- system (Export Profiles) on page 242
- traceoptions (Analytics) on page 243


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 89
- analytics on page 225
- *show analytics collector*


Copyright © 2016, Juniper Networks, Inc.

## analytics

**Syntax** *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;
      }
    }
}
```


Copyright © 2016, Juniper Networks, Inc.

*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;
  }
}
```

**Hierarchy Level** [edit services]

**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.

Copyright © 2016, Juniper Networks, Inc.

**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.

**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 on page 89
- *show analytics traffic-statistics*
- *show analytics collector*
- *show analytics status*
- *show analytics queue-statistics*
- *show analytics configuration*

 Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 on page 89

Copyright © 2016, Juniper Networks, Inc.

## 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 on page 89
- analytics on page 225
- latency-threshold on page 237
- resource-profiles (Analytics) on page 240


Copyright © 2016, Juniper Networks, Inc.

## 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.

Copyright © 2016, Juniper Networks, Inc.

- **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:

  http://www.juniper.net/techpubs/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.

**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 on page 89
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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:** ***x*m** 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. |

Copyright © 2016, Juniper Networks, Inc.

| | |
|---|---|
| 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 on page 89
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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.

Copyright © 2016, Juniper Networks, Inc.

**Related Documentation**

- Network Analytics Overview on page 89
- analytics on page 225

## 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**

- Network Analytics Overview on page 89
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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)

Copyright © 2016, Juniper Networks, Inc.

- 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 on page 89
- analytics on page 225
- depth-threshold on page 230

## 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.

**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 on page 89
- collector (Analytics) on page 229


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 on page 89
- analytics on page 225

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 on page 89
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 89
- analytics on page 225

Copyright © 2016, Juniper Networks, Inc.

## 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 on page 89
- analytics on page 225


Copyright © 2016, Juniper Networks, Inc.

## 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 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for 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:** *x***m** 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 on page 89
- analytics on page 225

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 15

# SNMP


- address on page 248
- address-mask on page 248
- agent-address on page 249
- alarm (SNMP RMON) on page 250
- authorization on page 251
- bucket-size on page 251
- categories on page 252
- client-list on page 252
- client-list-name on page 253
- clients on page 253
- commit-delay on page 254
- community (SNMP) on page 255
- community on page 256
- community-name on page 257
- contact (SNMP) on page 258
- description on page 258
- description on page 259
- destination-port on page 259
- engine-id on page 260
- event on page 261
- falling-event-index on page 261
- falling-threshold on page 262
- falling-threshold on page 263
- falling-threshold-interval on page 264
- filter-duplicates on page 264
- filter-interfaces on page 265
- group (Configuring Group Name) on page 266
- group (Defining Access Privileges for an SNMPv3 Group) on page 267


Copyright © 2016, Juniper Networks, Inc.

- health-monitor on page 267
- history on page 268
- interface (SNMP RMON History) on page 269
- interface (SNMP) on page 269
- interval on page 270
- interval on page 270
- interval on page 271
- location (SNMP) on page 271
- logical-system on page 272
- message-processing-model on page 273
- name on page 273
- nonvolatile on page 274
- notify on page 275
- notify-filter (Applying to the Management Target) on page 276
- notify-filter (Configuring the Profile Name) on page 276
- notify-view on page 277
- oid on page 277
- oid on page 278
- owner on page 278
- parameters on page 279
- port on page 279
- read-view on page 280
- request-type on page 281
- rising-event-index on page 282
- rising-threshold on page 283
- rising-threshold on page 284
- rmon on page 284
- rmon on page 285
- routing-instance on page 286
- routing-instance on page 287
- sample-type on page 287
- security-level (Defining Access Privileges) on page 288
- security-level (Generating SNMP Notifications) on page 289
- security-model (Access Privileges) on page 290
- security-model (Group) on page 291
- security-model (SNMP Notifications) on page 291
- security-name (Security Group) on page 292



Copyright © 2016, Juniper Networks, Inc.

- security-name (Community String) on page 293
- security-name (SNMP Notifications) on page 294
- security-to-group on page 295
- snmp on page 295
- snmp on page 296
- snmp-community on page 296
- source-address on page 297
- startup-alarm on page 298
- syslog-subtag on page 298
- tag on page 299
- tag-list on page 299
- target-address on page 300
- target-parameters on page 301
- targets on page 302
- traceoptions (SNMP) on page 303
- trap-group on page 305
- trap-options on page 306
- type on page 307
- type on page 308
- v3 on page 309
- vacm on page 311
- variable on page 312
- version (SNMP) on page 312
- view (Associating a MIB View with a Community) on page 313
- view (Configuring a MIB View) on page 314
- write-view on page 315


Copyright © 2016, Juniper Networks, Inc. 

## 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*

## 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*


Copyright © 2016, Juniper Networks, Inc.

## agent-address

**Syntax** agent-address outgoing-interface;

**Hierarchy Level** [edit snmp trap-options]

**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 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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*
- event on page 261
- *RMON MIB Event, Alarm, Log, and History Control Tables*
- *Monitoring RMON MIB Tables*
- *Understanding RMON*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## bucket-size

**Syntax** bucket-size *number*;

**Hierarchy Level** [edit snmp rmon history]

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

**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**
- Configuring SNMP (J-Web Procedure) on page 121
- *Junos OS Network Management Configuration Guide*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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** ***category***—Name of a trap type: **authentication**, **chassis**, **configuration**, **link**, **remote-operations**, **rmon-alarm**, **routing**, **services**, **sonet-alarms**, **startup**, or **vrrp-events**.

**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*

## client-list

**Syntax**
```
client-list client-list-name {
  ip-addresses;
}
```

**Hierarchy Level** [edit snmp]

**Release Information** Statement 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 QFX 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*


Copyright © 2016, Juniper Networks, Inc.

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

**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*

## clients

**Syntax**
```
clients {
  address <restrict>;
}
```

**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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## commit-delay

**Syntax** commit-delay *seconds*;

**Hierarchy Level** [edit snmp nonvolatile]

**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 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*


Copyright © 2016, Juniper Networks, Inc.

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

**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.

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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## contact (SNMP)

**Syntax** contact *contact*;

**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** Define the value of the 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*

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring an RMON Event Entry and Its Attributes*

## destination-port

**Syntax** destination-port *port-number*;

**Hierarchy Level** [edit snmp trap-group]

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

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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**—The engine ID suffix is generated from the default IP address.

**use-mac-address**—The SNMP engine identifier is generated from the MAC address of the management interface on the router.

**Default:** use-default-ip-address

**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 on page 124

 Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*
- alarm (SNMP RMON) on page 250

## 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*
- rising-event-index on page 282

Copyright © 2016, Juniper Networks, Inc.

## falling-threshold

**Syntax** falling-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.

**Description** The lower threshold is expressed as a percentage of the maximum possible value 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. 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**.

**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*
- rising-threshold on page 283

 Copyright © 2016, Juniper Networks, Inc.

## 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** The lower 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 startup-alarm value is equal to falling-alarm value or rising-or-falling-alarm value. 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**.

**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*
- rising-threshold on page 284

Copyright © 2016, Juniper Networks, Inc.

## 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** Interval between samples when the rising threshold is crossed. Once the alarm crosses 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*
- interval on page 271

## filter-duplicates

**Syntax** filter-duplicates;

**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** 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*


Copyright © 2016, Juniper Networks, Inc.

## filter-interfaces

**Syntax**

```
filter-interfaces {
  interfaces {
    all-internal-interfaces;
    interface 1;
    interface 2;
  }
}
```

**Hierarchy Level** [edit snmp]

**Release Information** Statement introduced in Junos OS Release 9.4 for EX Series Switches.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## 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 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure health monitoring.

The remaining statements are explained separately.

**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*

Copyright © 2016, Juniper Networks, Inc.

## history

**Syntax**

```
history history-index {
  bucket-size number;
  interface (SNMP RMON History) 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.

**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. It 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. The interface (SNMP RMON History) ***interface-name*** statement is mandatory. Other statements in the history group are optional.

**Default** Not configured.

**Options** ***history-index***—Identifies this history entry as an integer.

**Range:** 1 through 655535

**Required Privilege Level** snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

**Related Documentation**

- Configuring SNMP (J-Web Procedure) on page 121
- *Junos OS Network Management Configuration Guide*

 Copyright © 2016, Juniper Networks, Inc.

## 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.

**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**
- Configuring SNMP (J-Web Procedure) on page 121
- *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*

Copyright © 2016, Juniper Networks, Inc.

## interval

**Syntax** interval *seconds*;

**Hierarchy Level** [edit snmp rmon history]

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

**Description** Configure the interval over which data is to be sampled for the specified interface.

**Default** 1800 sec

**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.

## interval

**Syntax** interval *seconds*;

**Hierarchy Level** [edit snmp health-monitor]

**Release Information** Statement introduced in Junos OS Release 8.0.
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 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## location (SNMP)

**Syntax** location *location*;

**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** 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the Trap Target Address*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## name

**Syntax** name *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** 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*

Copyright © 2016, Juniper Networks, Inc.

## nonvolatile

**Syntax**

```
nonvolatile {
  commit-delay seconds;
}
```

**Hierarchy Level** [edit snmp]

**Release Information** Statement introduced before Junos OS Release 7.4.
The commit-delay statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure options for SNMP **Set** requests.

The statement is explained separately.

**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*
- commit-delay on page 254

 Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the SNMPv3 Trap Notification*

Copyright © 2016, Juniper Networks, Inc.

## 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*

## 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.

**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*
- oid on page 277

 Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the Notify View*

## oid

**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.

**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.

**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**
- *Configuring the Trap Notification Filter*

Copyright © 2016, Juniper Networks, Inc.

## oid

**Syntax** oid *object-identifier* (exclude | include);

**Hierarchy Level** [edit snmp view *view-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 an object identifier (OID) used to represent a subtree of MIB objects.

**Options** **exclude**—Exclude the subtree of MIB objects represented by the specified OID.

**include**—Include the subtree of MIB objects represented by the specified OID.

***object-identifier***—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

**Related Documentation**
- *Configuring MIB Views*

## 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.

**Description** Specify the user or group responsible for this 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**
- Configuring SNMP (J-Web Procedure) on page 121
- *Junos OS Network Management Configuration Guide*

 Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring MIB Views*


Copyright © 2016, Juniper Networks, Inc.

## 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*
- variable on page 312

Copyright © 2016, Juniper Networks, Inc.

## 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*
- falling-event-index on page 261

 Copyright © 2016, Juniper Networks, Inc.

## rising-threshold

**Syntax** 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.

**Description** The upper threshold is expressed as a percentage of the maximum possible value 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. 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**.

**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 on page 262
- *Configuring the Falling Threshold or Rising Threshold*

Copyright © 2016, Juniper Networks, Inc.

## 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** Upper 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 startup alarm value is equal to the falling alarm or rising or falling alarm value. 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.

**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*
- falling-threshold on page 263

## 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*


Copyright © 2016, Juniper Networks, Inc.

## rmon

**Syntax**

```
rmon {
  history history-index {
    interface (SNMP RMON History) interface-name;
    bucket-size number;
    interval seconds;
    owner owner-name;
  }
}
```

**Hierarchy Level** [edit snmp]

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

**Description** RMON is an existing feature of Junos OS.

The RMON specification provides network administrators with comprehensive network fault diagnosis, planning, and performance tuning information. It 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 RMON Statistics, History, Alarm, and Event groups. The EX Series documentation describes only the **rmon history** statement, which was added with this release.

The statements are explained separately.

**Default** Disabled.

**Required Privilege Level** snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

**Related Documentation**

- Configuring SNMP (J-Web Procedure) on page 121
- *Junos OS Network Management Configuration Guide*

Copyright © 2016, Juniper Networks, Inc. 

## routing-instance

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit snmp community *community-name*],
[edit snmp community *community-name* logical-system *logical-system-name*],
[edit snmp trap-group *group*]

**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*
- *Configuring the Source Address for SNMP Traps*
- *Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*

## snmp

**Syntax** snmp { ... }

**Hierarchy Level** [edit]

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

**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*

Copyright © 2016, Juniper Networks, Inc.

## snmp

**Syntax**

```
snmp {
  rmon {
    history index {
      interface (SNMP RMON History) interface-name;
      bucket-size number;
      interval seconds;
      owner owner-name;
    }
  }
}
```

**Hierarchy Level** [edit]

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

**Description** Configure SNMP.

The statements are explained separately.

**Required Privilege Level** snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

**Related Documentation**

- Configuring SNMP (J-Web Procedure) on page 121

## 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.

**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*


Copyright © 2016, Juniper Networks, Inc.

## source-address

**Syntax** source-address *address*;

**Hierarchy Level** [edit snmp trap-options]

**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 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*

Copyright © 2016, Juniper Networks, Inc.

## 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 Sample Type*

## 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*


Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the SNMPv3 Trap Notification*

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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*


Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Applying Target Parameters*

Copyright © 2016, Juniper Networks, Inc.

## targets

**Syntax**

```
targets {
  address;
}
```

**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.

**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*


Copyright © 2016, Juniper Networks, Inc.

## 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.

Copyright © 2016, Juniper Networks, Inc.

- **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*


Copyright © 2016, Juniper Networks, Inc.

## trap-group

**Syntax**

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  routing-instance instance;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

**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 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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## trap-options

**Syntax**

```
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
```

**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** 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.

The remaining statements are explained separately.

**Default** Disabled

**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*


Copyright © 2016, Juniper Networks, Inc.

## 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*

Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the SNMPv3 Trap Notification*


Copyright © 2016, Juniper Networks, Inc.

## 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;
        }
```

Copyright © 2016, Juniper Networks, Inc.

```
            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.


Copyright © 2016, Juniper Networks, Inc.

**Description** Configure SNMPv3.

The remaining statements are explained separately.

**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*

## 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.

**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*

Copyright © 2016, Juniper Networks, Inc.

## 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*

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

**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*


Copyright © 2016, Juniper Networks, Inc.

## view (Associating a MIB View with a Community)

**Syntax** view *view-name*;

**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.

**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*

Copyright © 2016, Juniper Networks, Inc.

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

**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.

**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*
- *Associating MIB Views with an SNMP User Group*
- community on page 255


Copyright © 2016, Juniper Networks, Inc.

## 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*
- *Configuring the Write View*

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

PART 3

# Operational Commands


- Realtime Performance Monitoring on page 319
- General Commands on page 331
- Analyzers and Port Mirroring on page 357
- sFlow Monitoring Technology on page 361
- Ethernet OAM Connectivity Fault Management on page 369
- Ethernet OAM Link Fault Management on page 409
- Uplink Failure Detection on page 415
- SNMP on page 419


Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 16

# Realtime Performance Monitoring

- show services rpm active-servers
- show services rpm history-results
- show services rpm probe-results

Copyright © 2016, Juniper Networks, Inc.

## 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.

**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 320

**Output Fields** Table 17 on page 320 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 17: 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
```


Copyright © 2016, Juniper Networks, Inc.

## show services rpm history-results

**Syntax**
show services rpm history-results
<brief | detail>
<owner *owner*>
<since *time*>
<test *name*>

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport routers.

**Description**
Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) instance.

**Options**
**none**—Display the results of the last 50 probes for all RPM instances.

**brief | detail**—(Optional) Display the specified level of output.

**owner *owner***—(Optional) Display information for the specified probe owner.

**since *time***—(Optional) Display information from the specified time. Specify time as ***yyyy-mm-dd.hh:mm:ss***.

**test *name***—(Optional) Display information for the specified test.

**Required Privilege Level**
view

**List of Sample Output**
show services rpm history-results on page 322
show services rpm history-results detail on page 322

**Output Fields**
Table 18 on page 321 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 18: 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:<br>• **Response received**—Timestamp when the probe result was determined.<br>• **Rtt**—Average ping round-trip time (RTT), in microseconds. | **detail** |

Copyright © 2016, Juniper Networks, Inc.

Table 18: 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:<br>• **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.<br>• **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.<br>• **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test.<br>• **Jitter**—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test.<br>• **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

```
user@host> show services rpm history-results
     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 detail

```
user@host> show services rpm history-results 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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```

Copyright © 2016, Juniper Networks, Inc.

## show services rpm probe-results

**Syntax**
show services rpm probe-results
<owner *owner*>
<test *name*>

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Series routers.

**Description**
Display the results of the most recent real-time performance monitoring (RPM) probes.

**Options**
**none**—Display all results of the most recent RPM probes.

**owner *owner***—(Optional) Display information for the specified probe owner.

**test *name***—(Optional) Display information for the specified test.

**Required Privilege Level**
view

**List of Sample Output**
show services rpm probe-results (IPv4 Targets) on page 327
show services rpm probe-results (IPv6 Targets) on page 329
show services rpm probe-results (BGP Neighbor Discovery) on page 330

**Output Fields**
Table 19 on page 324 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 19: show services rpm probe-results Output Fields

| Field Name | Field Description |
|---|---|
| **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.** |
| **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. |
| **Target address** | Destination IPv4 address used for the probes. This field is displayed when the probes are sent to the configured IPv4 targets or RPM servers. |
| **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. |
| **Source address** | Source address used for the probes. |
| **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**. |


Copyright © 2016, Juniper Networks, Inc.

Table 19: show services rpm probe-results Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Test size** | Number of probes within a test. |
| **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:<br>• 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**.<br>• 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.<br>• 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**. |
| **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:<br>• **Response received**—Timestamp when the probe result was determined.<br>• **Client and server hardware timestamps**—If timestamps are configured, an entry appears at this point.<br>• **Rtt**—Average ping round-trip time (RTT), in microseconds.<br>• **Egress jitter**—Egress jitter, in microseconds.<br>• **Ingress jitter**—Ingress jitter, in microseconds.<br>• **Round trip jitter**—Round-trip jitter, in microseconds.<br>• **Egress interarrival jitter**—Egress interarrival jitter, in microseconds.<br>• **Ingress interarrival jitter**—Ingress interarrival jitter, in microseconds.<br>• **Round trip interarrival jitter**—Round-trip interarrival jitter, in microseconds. |

Copyright © 2016, Juniper Networks, Inc.

Table 19: show services rpm 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.<br>• **Probes sent**—Number of probes sent within the current test.<br>• **Probes received**—Number of probe responses received within the current test.<br>• **Loss percentage**—Percentage of lost probes for the current test.<br>• **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.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |
| **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<br>• **Probes sent**—Number of probes sent for the most recently completed test.<br>• **Probes received**—Number of probe responses received for the most recently completed test.<br>• **Loss percentage**—Percentage of lost probes for the most recently completed test.<br>• **Test completed**—Time the most recent test was completed.<br>• **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.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |


Copyright © 2016, Juniper Networks, Inc.

Table 19: show services rpm 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.<br>• **Probes sent**—Number of probes sent in all tests.<br>• **Probes received**—Number of probe responses received in all tests.<br>• **Loss percentage**—Percentage of lost probes in all tests.<br>• **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.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |
| **Error Stats** | Displays error statistics for each probe.<br>• **Invalid client recv timestamp**—Number of client receive timestamp less than client send timestamp.<br>• **Invalid server send timestamp**—Number of server send timestamp less than server receive timestamp.<br>• **Invalid server processing time**—Number of server side spent time greater than RTT.<br>NOTE: **Error Stats** is displayed in the output only if non-zero statistics exists. |

## 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, 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
```

Copyright © 2016, Juniper Networks, Inc.

```
  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
```


Copyright © 2016, Juniper Networks, Inc.

```
        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, 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
```

Copyright © 2016, Juniper Networks, Inc.

```
    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 (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, 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
```


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 17

# General Commands

- monitor traffic
- ping
- show pfe statistics bridge
- traceroute

Copyright © 2016, Juniper Networks, Inc.

## 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>
<resolve-timeout>
<size size>
```

**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 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.

**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.


Copyright © 2016, Juniper Networks, Inc.

**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.

**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.

**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 20 on page 334.

Copyright © 2016, Juniper Networks, Inc.

Table 20: Match Conditions for the monitor traffic Command

| Match Type | Condition | Description |
|---|---|---|
| Entity | **host** [*address* \| *hostname*] | Matches packets that contain the specified address or hostname.<br><br>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.<br><br>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). |
| 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. |


Copyright © 2016, Juniper Networks, Inc.

Table 20: 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. |
| | **tcp** | Matches all TCP datagrams. |
| | **udp** | Matches all UDP datagrams. |

To combine expressions, use the logical operators listed in Table 21 on page 336.

Copyright © 2016, Juniper Networks, Inc.

Table 21: 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 22 on page 337.

 Copyright © 2016, Juniper Networks, Inc.

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 20 on page 334.
- 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 **ae0**) only shows inbound traffic data, the command does not show VLAN tag information in the output.

### Table 22: 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. |
| >= | 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. |

Copyright © 2016, Juniper Networks, Inc.

Table 22: Arithmetic and Relational Operators for the monitor traffic Command *(continued)*

| Arithmetic or Relational Operator | Description |
|---|---|
| = | 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 338
monitor traffic detail count on page 338
monitor traffic extensive (Absolute Sequence) on page 339
monitor traffic extensive (Relative Sequence) on page 339
monitor traffic extensive count on page 339
monitor traffic interface on page 339
monitor traffic matching on page 340
monitor traffic (TX Matrix Plus Router) on page 340
monitor traffic (QFX3500 Switch) on page 341
monitor traffic matching icmp on page 341
monitor traffic matching IP protocol number on page 342
monitor traffic matching arp on page 342
monitor traffic matching port on page 343

**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)
```


Copyright © 2016, Juniper Networks, Inc.

### 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

```
user@host>  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
```

Copyright © 2016, Juniper Networks, Inc.

```
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: .
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

## 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
...
```

Copyright © 2016, Juniper Networks, Inc.

## ping

List of Syntax
Syntax on page 344
Syntax (QFX Series) on page 344

Syntax

```
ping host
<bypass-routing>
<count requests>
<detail>
<do-not-fragment>
<inet | inet6>
<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>
<vpls instance-name>
<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>
```


Copyright © 2016, Juniper Networks, Inc.

<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.

**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.

**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) 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 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.

Copyright © 2016, Juniper Networks, Inc.

**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.

**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.

 Copyright © 2016, Juniper Networks, Inc.

**Required Privilege Level** network

**Related Documentation**
- *Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages*

**List of Sample Output**
ping hostname on page 347
ping hostname rapid on page 347
ping hostname size count on page 347

**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.

## Sample Output

### 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
```

Copyright © 2016, Juniper Networks, Inc.

## 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 System Process Information*
- *Monitoring Switch Control Traffic*

**List of Sample Output**
show pfe statistics bridge (EX3200 and EX4200 Switches) on page 349
show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis) on page 350
show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis) on page 351
show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card) on page 351

**Output Fields**
Table 23 on page 348 lists the output fields for the **show pfe statistics bridge** command. Output fields are listed in the approximate order in which they appear.

### Table 23: show pfe statistics bridge Output Fields

| Field Name | Field Description |
|---|---|
| **Ingress Counters** | Information about ingress counters:<br>• **Received**—Number of packets received by the bridge.<br>• **VLAN Filtered**—Number of packets discarded because of VLAN filtering.<br>• **Security Filtered**—Number of packets discarded because of security filtering.<br>• **Other Discards**—Number of packets dropped by the bridge for reasons other than VLAN or security filtering. |


Copyright © 2016, Juniper Networks, Inc.

Table 23: show pfe statistics bridge Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Egress Counters** | Information about egress counters:<br>• **Unicast**—Number of unicast packets transmitted.<br>• **Multicast**—Number of multicast packets transmitted.<br>• **Broadcast**—Number of broadcast packets transmitted.<br>• **Egress Filtered**—Number of egress-filtered packets (regardless of port, priority, or mode).<br>• **TailDrop**—Number of packets filtered because of egress queue congestion.<br>• **Forward Restrict**—Number of packets filtered because of egress forward restrictions.<br>• **Congestion Filtered**—Number of packets filtered because of transmit queue (TxQ) congestion.<br>• **Control Packets**—Number of control packets (sent to CPU, received from CPU, and sent to analyzer). |
| **Drop Counters** | Information about drop counters:<br>• **Drop Mode**—Count mode of the counter.<br>• **Drop Counter**—Counter value. |
| **General Counters** | Information about general counters:<br>• **Drop Mode**—Count mode of the counter.<br>• **Drop Counter**—Counter value.<br>• **Source Not Learnt**—Number of source addresses that were not learnt because of internal congestion. |
| **MUX PFE** | Information about multiplexer PFE for oversubscribed cards:<br>• **Drop Mode**—Count mode of the counter.<br>• **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
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

## traceroute

**List of Syntax**

Syntax on page 353
Syntax (QFX Series and OCX Series) on page 353

**Syntax**

traceroute *host*
<as-number-lookup>
<bypass-routing>
<clns>
<gateway *address*>
<inet | inet6>
<interface *interface-name*>
<logical system *logical-system-name*>
<monitor *host*>
<mpls (ldp *FEC address* | rsvp *label-switched-path-name*)>
<no-resolve>
<propagate-ttl>
<routing-instance *routing-instance-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*>
<no-resolve>
<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 16.1.

**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.

Copyright © 2016, Juniper Networks, Inc.

**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.

**clns**—(Optional) Trace the route belonging to Connectionless Network Service (CLNS).

**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) Perform this operation on all logical systems or on a particular logical system.

**monitor *host***—(Optional) Display real-time monitoring information for the specified host.

**monitor*host***—(Optional) Perform this operation to display real-time monitoring information.

**monitor*host***—(Optional) Perform this operation to display real-time monitoring information.

**monitor*host***—(Optional) Perform this operation to display real-time monitoring information.

**mpls (ldp *FEC address* | rsvp *label-switched-path name*)**—(Optional) See ***traceroute mpls ldp*** and ***traceroute mpls rsvp***.

**no-resolve**—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

**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.


Copyright © 2016, Juniper Networks, Inc.

**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.

**Required Privilege Level** network

**Related Documentation**
- *traceroute monitor*

**List of Sample Output**
traceroute on page 355
traceroute as-number-lookup host on page 356
traceroute no-resolve on page 356
traceroute propogate-ttl on page 356
traceroute (Between CE Routers, Layer 3 VPN) on page 356
traceroute (Through an MPLS LSP) on page 356

**Output Fields** Table 24 on page 355 describes the output fields for the **traceroute** command. Output fields are listed in the approximate order in which they appear.

Table 24: 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
```

Copyright © 2016, Juniper Networks, Inc.

### 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
```


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 18

# Analyzers and Port Mirroring

- show analyzer

Copyright © 2016, Juniper Networks, Inc.

## 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

**Related Documentation**
- *Understanding Port Mirroring on EX Series Switches*

**List of Sample Output** show analyzer on page 358

**Output Fields** Table 25 on page 358 lists the output fields for the **command-name** command. Output fields are listed in the approximate order in which they appear.

### Table 25: 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
```


Copyright © 2016, Juniper Networks, Inc.

```
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
```

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 19

# sFlow Monitoring Technology

- show sflow
- show sflow interface
- show sflow collector
- clear sflow collectors statistics

Copyright © 2016, Juniper Networks, Inc.

## show sflow

**Syntax**
show sflow
<collector>
<interface>

**Release Information**
Command introduced in Junos OS Release 9.3 for EX Series switches.

**Description**
Display default sFlow technology configuration information.

**Options**
**none**—Display default sFlow technology configuration information.

**collector**—(Optional) Display standard status information about the specified sFlow collector.

**interface**—(Optional) Display standard status information about the specified sFlow interface.

**Required Privilege Level**
view

**Related Documentation**
- show sflow interface on page 364
- show sflow collector on page 366
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

**List of Sample Output**
show sflow on page 363

**Output Fields**
Table 26 on page 362 lists the output fields for the **show sflow** command. Output fields are listed in the approximate order in which they appear.

### Table 26: show sflow Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **sFlow** | Status of the feature: **enabled** or **disabled**. | 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 |
| **Sample limit** | Number of packets sampled per second. The sampling limit cannot be configured and is set to 300 packets per second. | All levels |
| **Polling interval** | Interval at which the sFlow agent polls the interface. | All levels |
| **Agent ID** | The IP address assigned to the sFlow agent. | All levels |


Copyright © 2016, Juniper Networks, Inc.

Table 26: show sflow Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Source IP address** | The IP address for the sFlow datagram. | All levels |

## Sample Output

### show sflow

```
sFlow         : Enabled
Sample rate egress     : 1:1000
Sample rate ingress  : 1: 2048: Disabled
Sample limit     : 300 packets/second
Polling interval : 20 seconds
Agent ID    : 10.93.54.7
Source IP address : 10.93.54.7
```

Copyright © 2016, Juniper Networks, Inc.

## show sflow interface

**Syntax** show sflow interface

**Release Information** Command introduced in Junos OS Release 9.3 for EX Series switches.

**Description** Display the interfaces on which sFlow technology is enabled and the sampling parameters.

**Required Privilege Level** view

**Related Documentation**

- show sflow on page 362
- show sflow collector on page 366
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

**List of Sample Output** show sflow interface on page 364

**Output Fields** Table 27 on page 364 lists the output fields for the **show sflow interface** command. Output fields are listed in the approximate order in which they appear.

Table 27: show sflow interface Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Interface** | Interfaces on which sFlow technology is enabled. | All levels |
| **Status Egress** | Indicates whether egress sampling rate is enabled. | All levels |
| **Status Ingress** | Indicates whether ingress sampling 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** | The interval at which the sFlow agent polls the interface. | All levels |

### Sample Output

#### show sflow interface

```
Interface       Status     Sample rate    Adapted sample rate   Polling-interval
```


Copyright © 2016, Juniper Networks, Inc.

```
                Egress Ingress   Egress Ingress   Egress Ingress
ge-0/0/0.0      Enabled  Disabled  1000    2048    1000     2048           20
```

## show sflow collector

**Syntax** show sflow collector

**Release Information** Command introduced in Junos OS Release 9.3 for EX Series switches.

**Description** Display a list of configured sFlow collectors and their properties.

**Required Privilege Level** view

**Related Documentation**

- show sflow on page 362
- show sflow interface on page 364
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 60
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

**List of Sample Output** show sflow collector on page 366

**Output Fields** Table 28 on page 366 lists the output fields for the **show sflow collector** command. Output fields are listed in the approximate order in which they appear.

Table 28: show sflow collector Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **IP address** | IP address of the collector. | All levels |
| **UDP port** | UDP port number. | All levels |
| **No of samples** | Number of samples sent to collector. | All levels |

### Sample Output

#### show sflow collector

```
IP-address     UDP-Port  No of samples
10.204.32.46    5600    1000
100.204.32.76    3400    1000
```


Copyright © 2016, Juniper Networks, Inc.

## 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**

- show sflow collector on page 366
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 64

### Sample Output

clear sflow collectors statistics

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 20

# Ethernet OAM Connectivity Fault Management

- clear oam ethernet connectivity-fault-management delay-statistics
- clear oam ethernet connectivity-fault-management sla-iterator-statistics
- clear oam ethernet connectivity-fault-management statistics
- monitor ethernet delay-measurement
- show oam ethernet connectivity-fault-management delay-statistics
- show oam ethernet connectivity-fault-management forwarding-state
- show oam ethernet connectivity-fault-management interfaces
- show oam ethernet connectivity-fault-management path-database
- show oam ethernet connectivity-fault-management mep-database
- show oam ethernet connectivity-fault-management mip
- show oam ethernet connectivity-fault-management sla-iterator-statistics

Copyright © 2016, Juniper Networks, Inc.

## 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*
- show oam ethernet connectivity-fault-management delay-statistics on page 379
- *show oam ethernet connectivity-fault-management interfaces*

**List of Sample Output**

clear oam ethernet connectivity-fault-management delay statistics on page 370

**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
```


Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

## 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 372

**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
```

 Copyright © 2016, Juniper Networks, Inc.

## 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 on page 387
- show oam ethernet connectivity-fault-management path-database on page 393
- show oam ethernet connectivity-fault-management mip on page 402

**List of Sample Output** clear oam ethernet connectivity-fault-management statistics on page 373

**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
```

## 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.


Copyright © 2016, Juniper Networks, Inc.

**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)*
- show oam ethernet connectivity-fault-management mep-database on page 396
- ***show oam ethernet connectivity-fault-management mep-statistics***
- show oam ethernet connectivity-fault-management delay-statistics on page 379
- clear oam ethernet connectivity-fault-management statistics on page 373

**List of Sample Output**

monitor ethernet delay-measurement one-way on page 377
monitor ethernet delay-measurement two-way on page 377
monitor ethernet delay-measurement two-way (Invalid DMR Frames Received) on page 377

**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 29 on page 376 lists the run-time output fields for the **monitor ethernet delay-measurement one-way** command.
- Table 30 on page 376 lists the run-time output fields for the **monitor ethernet delay-measurement two-way** command.

Copyright © 2016, Juniper Networks, Inc.

Output fields are listed in the approximate order in which they appear.

### Table 29: 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 30: 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. |


Copyright © 2016, Juniper Networks, Inc.

Table 30: monitor ethernet delay-measurement two-way Output Fields *(continued)*

| Output Field Name | Output Field Description |
|---|---|
| **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 ---
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

## 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*
- clear oam ethernet connectivity-fault-management delay-statistics on page 370
- *show oam ethernet connectivity-fault-management interfaces*
- *show oam ethernet connectivity-fault-management mep-database*
- *show oam ethernet connectivity-fault-management mep-statistics*

**List of Sample Output** show oam ethernet connectivity-fault-management delay-statistics on page 381
show oam ethernet connectivity-fault-management delay-statistics remote-mep on page 381

**Output Fields** Table 31 on page 380 lists the output fields for the **show oam ethernet connectivity-fault-management delay-statistics** command and the **show oam ethernet**

Copyright © 2016, Juniper Networks, Inc.

**connectivity-fault-management mep-statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 31: 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.<br><br>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.<br><br>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. |


Copyright © 2016, Juniper Networks, Inc.

## 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
```


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 373
- show oam ethernet connectivity-fault-management path-database on page 393
- show oam ethernet connectivity-fault-management mip on page 402

**List of Sample Output**
show oam ethernet connectivity-fault-management forwarding-state on page 384
show oam ethernet connectivity-fault-management forwarding-state interface on page 384
show oam ethernet connectivity-fault-management forwarding-state interface detail on page 385
show oam ethernet connectivity-fault-management forwarding-state interface interface-name on page 386

**Output Fields** Table 32 on page 383 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 32: 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** |

Copyright © 2016, Juniper Networks, Inc.

Table 32: show oam ethernet connectivity-fault-management forwarding-state Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **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
```


Copyright © 2016, Juniper Networks, Inc.

```
  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
```


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 373
- show oam ethernet connectivity-fault-management path-database on page 393
- show oam ethernet connectivity-fault-management mip on page 402

**List of Sample Output**
show oam ethernet connectivity-fault-management interfaces on page 390
show oam ethernet connectivity-fault-management interfaces detail on page 390
show oam ethernet connectivity-fault-management interfacesextensive on page 391
show oam ethernet connectivity-fault-management interfaces level on page 392
show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces) on page 392

**Output Fields** Table 33 on page 387 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 33: 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** |

Copyright © 2016, Juniper Networks, Inc.

Table 33: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **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** |
| **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** |


Copyright © 2016, Juniper Networks, Inc.

Table 33: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **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** |
| **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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>For all other cases, this field displays **0**. | **detail extensive** |

Copyright © 2016, Juniper Networks, Inc.

Table 33: show oam ethernet connectivity-fault-management interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Valid DMRs received** | If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid DMRs received.<br><br>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.<br><br>For all other cases, this field displays **0**. | **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          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
```


Copyright © 2016, Juniper Networks, Inc.

```
    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
```


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 373
- show oam ethernet connectivity-fault-management interfaces on page 387
- show oam ethernet connectivity-fault-management mip on page 402

**List of Sample Output**

show oam ethernet connectivity-fault-management path-database on page 394
show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands) on page 394

**Output Fields** Table 34 on page 393 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 34: 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. |

Copyright © 2016, Juniper Networks, Inc.

Table 34: show oam ethernet connectivity-fault-management linktrace path-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **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
```


Copyright © 2016, Juniper Networks, Inc.

```
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 on page 373
- show oam ethernet connectivity-fault-management interfaces on page 387
- show oam ethernet connectivity-fault-management mip on page 402

**List of Sample Output**

show oam ethernet connectivity-fault-management mep-database on page 400
show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 400
show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event) on page 400

**Output Fields** Table 35 on page 396 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 35: show oam ethernet connectivity-fault-management mep-database Output Fields

| Field Name | Field Description |
|---|---|
| **Maintenance domain name** | Maintenance domain name. |


Copyright © 2016, Juniper Networks, Inc.

Table 35: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **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. |
| **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. |

Copyright © 2016, Juniper Networks, Inc.

Table 35: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **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. |
| **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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>For all other cases, this field displays **0**. |


Copyright © 2016, Juniper Networks, Inc.

Table 35: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Valid DMRs received** | If the MEP is an initiator for a two-way ETH-DM session: Number of valid DMRs received.<br><br>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.<br><br>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. |
| **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.<br>• In the Remote MEP section, displays the last value of port status TLV received from the remote MEP.<br>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.<br>• In the Remote MEP section, displays the last value of interface status TLV received from the remote MEP.<br>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. |

Copyright © 2016, Juniper Networks, Inc.

## 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
```


Copyright © 2016, Juniper Networks, Inc.

```
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)
```

Copyright © 2016, Juniper Networks, Inc.

## 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 on page 387
- show oam ethernet connectivity-fault-management path-database on page 393

**List of Sample Output** show oam ethernet connectivity-fault-management mip on page 402

**Output Fields** Table 36 on page 402 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 36: 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
```


Copyright © 2016, Juniper Networks, Inc.

## 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)*
- clear oam ethernet connectivity-fault-management sla-iterator-statistics on page 372

**List of Sample Output**

show oam ethernet connectivity-fault-management sla-iterator-statistics on page 406
show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) on page 406

**Output Fields**

Table 37 on page 403 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 37: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields

| Output Field Name | Output Field Description |
|---|---|
| **Maintenance domain** | Name of the maintenance domain. |

Copyright © 2016, Juniper Networks, Inc.

Table 37: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

| Output Field Name | Output Field Description |
|---|---|
| **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. |
| **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. |


Copyright © 2016, Juniper Networks, Inc.

Table 37: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

| Output Field Name | Output Field Description |
|---|---|
| **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. |
| **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. |

Copyright © 2016, Juniper Networks, Inc.

Table 37: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields *(continued)*

| Output Field Name | Output 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 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@switch> 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
```


Copyright © 2016, Juniper Networks, Inc.

```
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)
```

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 21

# Ethernet OAM Link Fault Management

- show oam ethernet link-fault-management

Copyright © 2016, Juniper Networks, Inc.

## 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 on EX Series Switches on page 76
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 83

**List of Sample Output**
show oam ethernet link-fault-management brief on page 414
show oam ethernet link-fault-management detail on page 414

**Output Fields**
Table 38 on page 410 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 38: show oam ethernet link-fault-management Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Status** | Indicates the status of the established link.<br>• **Fail**—A link fault condition exists.<br>• **Running**—A link fault condition does not exist. | All levels |
| **Discovery state** | State of the discovery mechanism:<br>• **Passive Wait**<br>• **Send Any**<br>• **Send Local Remote**<br>• **Send Local Remote Ok** | All levels |
| **Peer address** | Address of the OAM peer. | All levels |


Copyright © 2016, Juniper Networks, Inc.

Table 38: show oam ethernet link-fault-management Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Flags** | Information about the interface.<br>• **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.<br>• **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.<br>• **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 |
| **Remote entity information** | Remote entity information.<br>• **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.<br>• **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.<br>• **Discovery mode**—Indicates whether discovery mode is active or inactive.<br>• **Unidirectional mode**—Indicates the ability to operate a link in a unidirectional mode for diagnostic purposes.<br>• **Remote loopback mode**—Indicates whether remote loopback is supported or not supported.<br>• **Link events**—Indicates whether interpreting link events is supported or not supported on the remote peer.<br>• **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** |

Copyright © 2016, Juniper Networks, Inc.

Table 38: show oam ethernet link-fault-management Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **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** |
| **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.<br><br>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.<br><br>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** |


Copyright © 2016, Juniper Networks, Inc.

Table 38: 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.<br><br>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** |
| **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** |

Copyright © 2016, Juniper Networks, Inc.

## 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
```


Copyright © 2016, Juniper Networks, Inc.

CHAPTER 22

# Uplink Failure Detection

- show uplink-failure-detection

Copyright © 2016, Juniper Networks, Inc.

## 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) on page 87

**List of Sample Output** show uplink-failure-detection on page 416

**Output Fields** Table 39 on page 416 lists the output fields for the **show uplink-failure-detection** command. Output fields are listed in the approximate order in which they appear.

### Table 39: 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.<br>NOTE: The asterisk (*) indicates that the link is up. |
| Downlink | The downlink interface or interfaces configured as link-to-disable.<br>NOTE: The asterisk (*) indicates that the link is up. |
| Failure Action | Status of uplink failure detection:<br>• Active—The switch has detected an uplink failure and has brought the downlink down.<br>• 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
```


Copyright © 2016, Juniper Networks, Inc.

```
Group             : group2
Uplink            :  ge-0/0/3.0
Downlink          :  ge-0/0/4.0
Failure Action    :  Active
```

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 23

# SNMP


- clear snmp rmon history
- clear snmp statistics
- request snmp spoof-trap
- show snmp health-monitor
- show snmp inform-statistics
- show snmp mib
- show snmp rmon
- show snmp rmon history
- show snmp statistics
- show snmp v3


Copyright © 2016, Juniper Networks, Inc.

## clear snmp rmon history

**Syntax** **clear snmp rmon history <*interface-name* | all>**

**Release Information** Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Delete the samples of Ethernet statistics collected, but do not delete the RMON history configuration.

The **clear snmp rmon history** command deletes all the samples collected for the interface configured for the history group, but not the configuration of that group. If you want to delete the RMON history group configuration, you must use the **delete snmp rmon history** configuration-mode command.

**Options** ***interface-name***—Delete the samples of Ethernet statistics collected for this interface.

**all**—Delete the samples of Ethernet statistics collected for all interfaces that have been configured for RMON monitoring.

**Required Privilege Level** clear

**Related Documentation**

- show snmp rmon history on page 445

 Copyright © 2016, Juniper Networks, Inc.

## 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 on page 449

**List of Sample Output** clear snmp statistics on page 421

**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
```

 Copyright © 2016, Juniper Networks, Inc.

## 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 423
request snmp spoof-trap (Illegal Trap Name) on page 423
request snmp spoof-trap (Question Mark ?) on page 427

### 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
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

```
  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%)---
```


Copyright © 2016, Juniper Networks, Inc.

## 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 431
show snmp health-monitor alarms detail on page 433

**Output Fields** Table 40 on page 429 describes the output fields for the **show snmp health-monitor** command. Output fields are listed in the approximate order in which they appear.

Table 40: 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 |

Copyright © 2016, Juniper Networks, Inc.

Table 40: show snmp health-monitor Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **State** | State of the alarm or event entry:<br>• Alarms:<br>  • **active**—Entry is fully configured and activated.<br>  • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit.<br>  • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit.<br>  • **under creation**—Entry is being configured and is not yet activated.<br>  • **startup**—Alarm is waiting for the first sample of the monitored variable.<br>  • **object not available**—Monitored variable of that type is not available to the health monitor agent.<br>  • **instance not available**—Monitored variable's instance is not available to the health monitor agent.<br>  • **object type invalid**—Monitored variable is not a numeric value.<br>  • **object processing errored**—An error occurred when the monitored variable was processed.<br>  • **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** |
| **Startup alarm** | Alarm that might be sent when this entry is first activated, depending on the following criteria:<br>• Alarm is sent when one of the following situations exists:<br>  • 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.**<br>  • 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**.<br>• Alarm is *not* sent when one of the following situations exists:<br>  • Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.<br>  • Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.<br>  • 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** |


Copyright © 2016, Juniper Networks, Inc.

Table 40: show snmp health-monitor Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **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
```

Copyright © 2016, Juniper Networks, Inc.

```
      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
```


Copyright © 2016, Juniper Networks, Inc.

```
      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
```

Copyright © 2016, Juniper Networks, Inc.

```
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
```


Copyright © 2016, Juniper Networks, Inc.

```
    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 436

**Output Fields** Table 41 on page 436 describes the output fields for the **show snmp inform-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 41: 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. |
| **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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```

Copyright © 2016, Juniper Networks, Inc.

## show snmp mib

**Syntax** show snmp mib (get | get-next | walk) (ascii | decimal) *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.

**Description** Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.

**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.

**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.

***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 439
show snmp mib get (Multiple Objects) on page 439
show snmp mib get (Layer 2 Policer) on page 439
show snmp mib get-next on page 439
show snmp mib get-next (Specify an OID) on page 439
show snmp mib walk on page 439
show snmp mib walk (QFX Series) on page 439
show snmp mib walk decimal on page 440
show snmp mib walk (ASCII) on page 440
show snmp mib walk (Multiple Indices) on page 440
show snmp mib walk decimal (Multiple Indices) on page 440

**Output Fields** Table 42 on page 439 describes the output fields for the **show snmp mib** command. Output fields are listed in the approximate order in which they appear.


Copyright © 2016, Juniper Networks, Inc.

Table 42: 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 (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
```

Copyright © 2016, Juniper Networks, Inc.

```
sysName.0     = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

### show snmp mib walk decimal

```
user@host show snmp mib walk decimal jnxUtilData
jnxUtilCounter32Value.102.114.101.100 = 100
```

### show snmp mib walk (ASCII)

```
show snmp mib walk ascii jnxUtilData
jnxUtilCounter32Value."fred" = 100
```

### show snmp mib walk (Multiple Indices)

```
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 (Multiple Indices)

```
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
.......
```


Copyright © 2016, Juniper Networks, Inc.

## 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.

**Description**
Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms and events.

**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

**List of Sample Output**
show snmp rmon on page 443
show snmp rmon alarms detail on page 443
show snmp rmon events detail on page 444

**Output Fields**
Table 43 on page 441 describes the output fields for the **show snmp rmon** command. Output fields are listed in the approximate order in which they appear.

Table 43: show snmp rmon Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Alarm Index** | Alarm identifier. | All levels |

Table 43: show snmp rmon Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **State** | State of the alarm or event entry:<br><br>Alarms:<br><br>• **active**—Entry is fully configured and activated.<br>• **falling threshold crossed**—Value of the variable has crossed the lower threshold limit.<br>• **rising threshold crossed**—Value of the variable has crossed the upper threshold limit.<br>• **under creation**—Entry is being configured and is not yet activated.<br>• **startup**—Alarm is waiting for the first sample of the monitored variable.<br>• **object not available**—Monitored variable of that type is not available to the SNMP agent.<br>• **instance not available**—Monitored variable's instance is not available to the SNMP agent.<br>• **object type invalid**—Monitored variable is not a numeric value.<br>• **object processing errored**—An error occurred when the monitored variable was processed.<br>• **unknown**—State is not one of the above.<br><br>Events:<br><br>• **active**—Entry has been fully configured and activated.<br>• **under creation**—Entry is being configured and is not yet activated.<br>• **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 |
| **Type** | Type of notification made when an event is triggered. It can be one of the following:<br><br>• **log**—A system log message is generated and an entry is made to the log table.<br>• **snmptrap**—An SNMP trap is sent to the configured destination.<br>• **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.<br>• **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** | Identifies the 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** |


Copyright © 2016, Juniper Networks, Inc.

Table 43: show snmp rmon 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:<br>• Alarm is sent when one of the following situations exists:<br>  ◦ 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.**<br>  ◦ 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**.<br>• Alarm is *not* sent when one of the following situations exists:<br>  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.<br>  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.<br>  ◦ 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** |
| **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 alarms detail

```
user@host> show snmp rmon alarms detail
```

Copyright © 2016, Juniper Networks, Inc.

```
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:
  Type                                log and trap
  Community                           boy-elroy
  Last event                          2002-01-30 01:13:01 PST
  Creator                             CLI
  State                               active
```


Copyright © 2016, Juniper Networks, Inc.

## show snmp rmon history

**Syntax**
**show snmp rmon history**
*<history-index>*
*<sample-index>*

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**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***—(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 rmon history on page 420

**List of Sample Output**
show snmp rmon history 1 on page 446
show snmp rmon history 1 sample 15 on page 447

**Output Fields**
Table 44 on page 445 lists the output fields for the **show smp rmon history** command. Output fields are listed in the approximate order in which they appear.

### Table 44: 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. |

Copyright © 2016, Juniper Networks, Inc.

Table 44: show smp rmon history Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sample Index** | The sample statistics taken at the specified interval.<br>• **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.<br>• **Octets**—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type.<br>• **Packets**—Total number of packets.<br>• **Broadcast Packets**—Number of broadcast packets.<br>• **Multicast Packets**—Number of multicast packets.<br>• **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).<br>• **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.<br>• **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.<br>• **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.<br>• **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.<br>• **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.<br>• **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
```


Copyright © 2016, Juniper Networks, Inc.

```
    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 15

```
user@host> show snmp rmon history 1 sample 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
```

Copyright © 2016, Juniper Networks, Inc.

```
Collisions  = 0
Utilization (%)  = 0
```


Copyright © 2016, Juniper Networks, Inc.

## 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 on page 421

**List of Sample Output**
show snmp statistics on page 454
show snmp statistics subagents on page 454

**Output Fields**
Table 45 on page 450 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2016, Juniper Networks, Inc.

## Table 45: show snmp statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Input** | Information about received packets:<br>• **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service.<br>• **Bad versions—(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version.<br>• **Bad community names—(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity.<br>• **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.<br>• **ASN parse errors—(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.<br>• **Too bigs—(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**.<br>• **No such names—(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**.<br>• **Bad values—(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**.<br>• **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. |


Copyright © 2016, Juniper Networks, Inc.

Table 45: 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**.<br>• **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.<br>• **Total set varbinds—(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs.<br>• **Get requests—(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity.<br>• **Get nexts—(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity.<br>• **Set requests—(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity.<br>• **Get responses—(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity.<br>• **Traps—(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity.<br>• **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.<br>• **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.<br>• **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration.<br>• **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit. |

Copyright © 2016, Juniper Networks, Inc.

Table 45: show snmp statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **V3 Input** | Information about SNMP version 3 packets:<br>• **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.<br>• **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.<br>• **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.<br>• **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable.<br>• **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine.<br>• **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).<br>• **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.<br>• **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.<br>• **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.<br>• **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.<br>• **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted. |


Copyright © 2016, Juniper Networks, Inc.

Table 45: show snmp statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Output** | Information about transmitted packets:<br>• **Packets—(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service.<br>• **Too bigs—(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**.<br>• **No such names—(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**.<br>• **Bad values—(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**.<br>• **General errors—(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**.<br>• **Get requests—(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity.<br>• **Get nexts—(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity.<br>• **Set requests—(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity.<br>• **Get responses—(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity.<br>• **Traps—(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity. |

Table 46 on page 453 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 46: 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. |
| **Maximum Response Time** | Maximum time taken by the SNMP subagent to send the statistics response. |

Copyright © 2016, Juniper Networks, Inc.

## 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
```


Copyright © 2016, Juniper Networks, Inc.

```
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
```

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

## 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 459

**Output Fields**
Table 47 on page 458 describes the output fields for the **show snmp v3** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2016, Juniper Networks, Inc.

## Table 47: show snmp v3 Output Fields

| Field Name | Field Description |
|---|---|
| **Access control** | Information about access control:<br>• **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.<br>• **Context prefix**—SNMPv3 context for which the configured access privileges apply.<br>• **Security model/level**—Security model and security level for which the configuration access privileges apply.<br>• **Read view**—Identifies the MIB view applied to SNMPv3 read operations.<br>• **Write view**—Identifies the MIB view applied to SNMPv3 write operations.<br>• **Notify view**—Identifies the MIB view applied to outbound SNMP notifications. |
| **Engine** | Information about local engine configuration:<br>• **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.<br>• **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.<br>• **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.<br>• **Max msg size**—Maximum message size the sender can accommodate. |
| **Engine ID** | Information about engine ID:<br>• **Local engine ID**—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.<br>• **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.<br>• **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.<br>• **Max msg size**—Maximum message size the sender can accommodate.<br>• **Engine ID**—SNMPv3 engine ID associated with each user.<br>• **User**—SNMPv3 user.<br>• **Auth/Priv**—Authentication and encryption algorithm available for use by each user.<br>• **Storage**—Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.<br>• **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. |
| **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. |


Copyright © 2016, Juniper Networks, Inc.

## 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
```

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.