




Junos[®] OS for EX Series Ethernet Switches, Release 11.3: Network Management and Monitoring



Published: 2011-11-23
Revision 2

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® OS for EX Series Ethernet Switches, Release 11.3: Network Management and Monitoring
Copyright © 2011, Juniper Networks, Inc.
All rights reserved.

Revision History
November 2011—Revision 2
September 2011—Revision 1

The information in this document is current as of the date listed in the revision history.

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 This Topic Collection	xi
	How to Use This Guide	xi
	List of EX Series Guides for Junos OS Release 11.3	xi
	Downloading Software	xiii
	Documentation Symbols Key	xiv
	Documentation Feedback	xv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvi
Part 1	Network Management and Monitoring	
Chapter 1	Port Mirroring	3
	Port Mirroring—Overview	3
	Understanding Port Mirroring on EX Series Switches	3
	Port Mirroring Overview	4
	Port Mirroring Terminology	5
	Configuration Guidelines for Port Mirroring on the Switches	6
	Examples: Port Mirroring Configuration	9
	Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches	9
	Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches	14
	Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches	25
	Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches	34
	Configuring Port Mirroring	42
	Configuring Port Mirroring to Analyze Traffic (CLI Procedure)	42
	Configuring Port Mirroring for Local Traffic Analysis	43
	Configuring Port Mirroring for Remote Traffic Analysis	43
	Filtering the Traffic Entering an Analyzer	44
	Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)	46
	Verifying Port Mirroring Configuration	47
	Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches	47
	Configuration Statements for Port Mirroring	48
	[edit ethernet-switching-options] Configuration Statement Hierarchy	49
	analyzer	52
	egress	53
	egress (Interface or VLAN)	53

	ethernet-switching-options	54
	ingress	57
	ingress (Interface or VLAN)	57
	input	58
	interface	59
	loss-priority	60
	no-tag	60
	output	61
	ratio	62
	vlan	63
	Operational Commands for Port Mirroring	63
	show analyzer	64
Chapter 2	sFlow Monitoring Technology	67
	sFlow Technology—Overview	67
	Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch	67
	Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches	67
	Adaptive Sampling	68
	sFlow Agent Address Assignment	69
	Example: sFlow Technology Configuration	70
	Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches	70
	Configuring sFlow Technology	74
	Configuring sFlow Technology for Network Monitoring (CLI Procedure)	74
	Configuration Statements for sFlow Technology	76
	[edit protocols] Configuration Statement Hierarchy	76
	collector	84
	disable	84
	interfaces	85
	polling-interval	86
	sample-rate	87
	sflow	88
	udp-port	89
	Operational Commands for sFlow Technology	89
	show sflow	90
	show sflow collector	92
	show sflow interface	93
Chapter 3	SNMP	95
	Configuring SNMP	95
	Configuring SNMP (J-Web Procedure)	95
	Configuration Statements for SNMP	98
	[edit snmp] Configuration Statement Hierarchy	98
	address	99
	address-mask	99
	agent-address	100
	alarm	101
	authorization	102

bucket-size	102
categories	103
client-list	103
client-list-name	104
clients	104
commit-delay	105
community	106
community	107
community-name	108
contact	109
description	109
description	110
destination-port	110
engine-id	111
event	112
falling-event-index	112
falling-threshold	113
falling-threshold	114
falling-threshold-interval	115
filter-duplicates	115
filter-interfaces	116
group (Configuring Group Name)	117
group (Defining Access Privileges for an SNMPv3 Group)	118
health-monitor	118
history	119
interface	120
interface	120
interval	121
interval	121
interval	122
location	122
logical-system	123
message-processing-model	124
name	124
nonvolatile	125
notify	126
notify-filter (Configuring the Profile Name)	127
notify-filter (Applying to the Management Target)	127
notify-view	128
oid	128
oid	129
owner	129
parameters	130
port	130
read-view	131
request-type	132
rising-event-index	133
rising-threshold	134
rising-threshold	135

rmon	135
rmon	136
routing-instance	137
routing-instance	138
sample-type	138
security-level (Generating SNMP Notifications)	139
security-level (Defining Access Privileges)	140
security-model (Access Privileges)	141
security-model (Group)	142
security-model (SNMP Notifications)	142
security-name (Security Group)	143
security-name (Community String)	143
security-name (SNMP Notifications)	144
security-to-group	145
snmp	145
snmp	146
snmp-community	146
source-address	147
startup-alarm	148
syslog-subtag	148
tag	149
tag-list	149
target-address	150
target-parameters	151
targets	152
traceoptions	153
trap-group	155
trap-options	156
type	156
type	157
v3	158
vacm	160
variable	161
version	161
view (Configuring a MIB View)	162
view (Associating a MIB View with a Community)	163
write-view	163
Operational Commands for SNMP	163
clear snmp rmon history	164
clear snmp statistics	165
request snmp spoof-trap	167
show snmp health-monitor	173
show snmp inform-statistics	180
show snmp rmon	182
show snmp rmon history	186
show snmp statistics	190
show snmp v3	194

Chapter 4	Real-Time Performance Monitoring (RPM)	197
	RPM—Overview	197
	Understanding Real-Time Performance Monitoring on EX Series	
	Switches	198
	RPM Packet Collection	198
	Tests and Probe Types	198
	Hardware Timestamps	199
	Limitations of RPM on EX Series Switches	201
	Configuring Real-Time Performance Monitoring (RPM)	201
	Configuring Real-Time Performance Monitoring (J-Web Procedure)	201
	Configuring the Interface for RPM Timestamping for Client/Server on an EX	
	Series Switch (CLI Procedure)	208
	Verifying Real-Time Performance Monitoring	210
	Viewing Real-Time Performance Monitoring Information	210
	Configuration Statements for Real-Time Performance Monitoring	211
	data-fill	211
	data-size	212
	destination-port	213
	dscp-code-point	214
	hardware-timestamp	215
	history-size	215
	moving-average-size	216
	one-way-hardware-timestamp	216
	port (RPM)	217
	probe	218
	probe-count	219
	probe-interval	219
	probe-limit	220
	probe-server	220
	probe-type	221
	routing-instance	222
	routing-instances	222
	rpm	223
	source-address	223
	target	224
	tcp	224
	test	225
	test-interval	226
	thresholds	227
	traps	228
	udp	229
	Operational Commands for Real-Time Performance Monitoring	229
	show services rpm active-servers	230
	show services rpm history-results	231
	show services rpm probe-results	234

Chapter 5	Ethernet OAM Link Fault Management	241
	Ethernet OAM Link Fault Management—Overview	241
	Understanding Ethernet OAM Link Fault Management for an EX Series Switch	241
	Example of Ethernet OAM Link Fault Management Configuration	242
	Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches	243
	Configuring Ethernet OAM Link Fault Management	245
	Configuring Ethernet OAM Link Fault Management (CLI Procedure)	246
	Configuration Statements for Ethernet OAM Link Fault Management	248
	[edit protocols] Configuration Statement Hierarchy	248
	action	255
	action-profile	256
	allow-remote-loopback	257
	ethernet	258
	event	260
	event-thresholds	260
	frame-error	261
	frame-period	261
	frame-period-summary	262
	interface	263
	link-adjacency-loss	264
	link-discovery	264
	link-down	265
	link-event-rate	265
	link-fault-management	266
	negotiation-options	267
	no-allow-link-events	267
	oam	268
	pdu-interval	270
	pdu-threshold	270
	remote-loopback	271
	symbol-period	271
	syslog	272
	Operational Commands for Ethernet OAM Link Fault Management	272
	show oam ethernet link-fault-management	273
Chapter 6	Ethernet OAM Connectivity Fault Management	279
	Ethernet OAM Connectivity Fault Management—Overview	279
	Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch	279
	Example of Ethernet OAM Connectivity Fault Management Configuration	280
	Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches	281
	Configuring Ethernet OAM Connectivity Fault Management	284
	Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure)	284
	Creating the Maintenance Domain	285
	Configuring the Maintenance Domain MIP Half Function	285

Creating a Maintenance Association	286
Configuring the Continuity Check Protocol	286
Configuring a Maintenance Association End Point	286
Configuring a Connectivity Fault Management Action Profile	287
Configuring the Linktrace Protocol	288
Configuration Statements for Ethernet OAM Connectivity Fault Management	288
[edit protocols] Configuration Statement Hierarchy	288
action-profile (Applying to OAM CFM, for EX Series Switch Only)	296
age (EX Series Switch Only)	296
auto-discovery (EX Series Switch Only)	297
connectivity-fault-management (EX Series Switch Only)	298
continuity-check (EX Series Switch Only)	299
direction (EX Series Switch Only)	299
hold-interval (OAM CFM, for EX Series Switch Only)	300
interface (OAM CFM, for EX Series Switch Only)	300
interval (EX Series Switch Only)	301
level (EX Series Switch Only)	301
linktrace (EX Series Switch Only)	302
loss-threshold (EX Series Switch Only)	302
maintenance-association (EX Series Switch Only)	303
maintenance-domain (EX Series Switch Only)	304
mep (EX Series Switch Only)	305
mip-half-function (EX Series Switch Only)	306
name-format (EX Series Switch Only)	307
path-database-size (EX Series Switch Only)	307
remote-mep (EX Series Switch Only)	308
Operational Commands for Ethernet OAM Connectivity Fault Management	308
clear oam ethernet connectivity-fault-management statistics	309
show oam ethernet connectivity-fault-management forwarding-state	310
show oam ethernet connectivity-fault-management interfaces	314
show oam ethernet connectivity-fault-management linktrace path-database	320
show oam ethernet connectivity-fault-management mep-database	322
show oam ethernet connectivity-fault-management mip	328
Chapter 7 Uplink Failure Detection	329
Uplink Failure Detection—Overview	329
Understanding Uplink Failure Detection	329
Uplink Failure Detection Overview	329
Failure Detection Pair	330
Configuring Uplink Failure Detection	331
Configuring Interfaces for Uplink Failure Detection (CLI Procedure)	331
Verifying Uplink Failure Detection	332
Verifying That Uplink Failure Detection Is Working Correctly	332
Configuration Statements for Uplink Failure Detection	334
group	334
link-to-disable	334
link-to-monitor	335

	uplink-failure-detection	335
	Operational Commands for Uplink Failure Detection	335
	show uplink-failure-detection	336
Chapter 8	Monitoring General Network Traffic and Hosts	339
	Monitoring Hosts Using the J-Web Ping Host Tool	339
	Monitoring Network Traffic Using Traceroute	341
Chapter 9	Configuration Statements for General Network Management and Monitoring	343
	archive-sites	343
	class-usage-profile	344
	counters	345
	destination-classes	345
	fields (for Interface Profiles)	346
	file (Associating with a Profile)	347
	file (Configuring a Log File)	348
	files	349
	filter-profile	350
	interface-profile	351
	interval	352
	mib-profile	353
	object-names	354
	operation	354
	routing-engine-profile	355
	size	356
	source-classes	356
	start-time	357
	transfer-interval	357
Chapter 10	Operational Commands for General Network Management and Monitoring	359
	monitor traffic	360
	ping	369
	show snmp mib	373
	traceroute	376

About This Topic Collection

- [How to Use This Guide on page xi](#)
- [List of EX Series Guides for Junos OS Release 11.3 on page xi](#)
- [Downloading Software on page xiii](#)
- [Documentation Symbols Key on page xiv](#)
- [Documentation Feedback on page xv](#)
- [Requesting Technical Support on page xvi](#)

How to Use This Guide

Complete documentation for the EX Series product family is provided on webpages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html. We have selected content from these webpages and created a number of EX Series guides that collect related topics into a book-like format so that the information is easy to print and easy to download to your local computer.

Software features for EX Series switches are listed by platform and by Junos OS release in a standalone document. See [EX Series Switch Software Features Overview](#).

The release notes are at http://www.juniper.net/techpubs/en_US/junos11.3/information-products/topic-collections/release-notes/11.3/junos-release-notes-11.3.pdf.

List of EX Series Guides for Junos OS Release 11.3

Title	Description
<i>Complete Hardware Guide for EX2200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX2200 Ethernet switches
<i>Complete Hardware Guide for EX3200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 Ethernet switches
<i>Complete Hardware Guide for EX3300 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3300 Ethernet switches

Title	Description
<i>Complete Hardware Guide for EX4200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4200 Ethernet switches
<i>Complete Hardware Guide for EX4500 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4500 Ethernet switches
<i>Complete Hardware Guide for EX6210 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX6210 Ethernet switches
<i>Complete Hardware Guide for EX8208 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 Ethernet switches
<i>Complete Hardware Guide for EX8216 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 Ethernet switches
<i>Complete Hardware Guide for the XRE200 External Routing Engine</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for the XRE200 External Routing Engine
<i>Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3</i>	Software feature descriptions, configuration examples, and tasks for Junos OS for EX Series switches
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the <i>Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3.</i>)
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Access Control</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Configuration Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Class of Service</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Device Security</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Ethernet Switching</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: EX3300, EX4200, and EX4500 Virtual Chassis</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: EX8200 Virtual Chassis</i>	





Title	Description
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Fibre Channel over Ethernet</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: High Availability</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Interfaces</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Layer 3 Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: MPLS</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Multicast</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Network Management and Monitoring</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Port Security</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Power over Ethernet</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Routing Policy and Packet Filtering</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Software Installation</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Spanning-Tree Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Monitoring</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Services</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Setup</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: User and Access Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: User Interfaces</i>	

Downloading Software

You can download Junos OS for EX Series switches from the Download Software area at <http://www.juniper.net/customers/support/> . To download the software, you must

have a Juniper Networks user account. For information about obtaining an account, see <http://www.juniper.net/entitlement/setupAccountInfo.do>.

Documentation Symbols Key

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.
Text and Syntax Conventions		
Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.

Text and Syntax Conventions		
Convention	Description	Examples
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</code>
(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.	<code>broadcast multicast</code> <code>(<i>string1</i> <i>string2</i> <i>string3</i>)</code>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<code>rsvp { # Required for dynamic MPLS only</code>
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	<code>community name members [<i>community-ids</i>]</code>
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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. Send e-mail to techpubs-comments@juniper.net with the following:

- Document URL or title
- Page number if applicable
- Software version
- Your name and company

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 JNASC 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/>
- 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: <https://www.juniper.net/alerts/>
- 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> .

PART 1

Network Management and Monitoring

- [Port Mirroring on page 3](#)
- [sFlow Monitoring Technology on page 67](#)
- [SNMP on page 95](#)
- [Real-Time Performance Monitoring \(RPM\) on page 197](#)
- [Ethernet OAM Link Fault Management on page 241](#)
- [Ethernet OAM Connectivity Fault Management on page 279](#)
- [Uplink Failure Detection on page 329](#)
- [Monitoring General Network Traffic and Hosts on page 339](#)
- [Configuration Statements for General Network Management and Monitoring on page 343](#)
- [Operational Commands for General Network Management and Monitoring on page 359](#)

CHAPTER 1

Port Mirroring

- [Port Mirroring—Overview on page 3](#)
- [Examples: Port Mirroring Configuration on page 9](#)
- [Configuring Port Mirroring on page 42](#)
- [Verifying Port Mirroring Configuration on page 47](#)
- [Configuration Statements for Port Mirroring on page 48](#)
- [Operational Commands for Port Mirroring on page 63](#)

Port Mirroring—Overview

- [Understanding Port Mirroring on EX Series Switches on page 3](#)

Understanding Port Mirroring on EX Series Switches

You can use port mirroring to facilitate analyzing traffic on your Juniper Networks EX Series Ethernet Switch on a packet level. You might use port mirroring as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing and for identifying sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

Port mirroring copies 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 Juniper Networks EX2200, EX3200, EX4200, or EX4500 Ethernet Switches
- Packets exiting a VLAN on Juniper Networks EX8200 Ethernet Switches

This topic describes:

- [Port Mirroring Overview on page 4](#)
- [Port Mirroring Terminology on page 5](#)
- [Configuration Guidelines for Port Mirroring on the Switches on page 6](#)

Port Mirroring Overview

Port 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.

You configure port mirroring on the switch to send copies of unicast traffic to either a local analyzer port or an analyzer VLAN. Then you can analyze the mirrored traffic using a protocol analyzer application. The protocol analyzer application can run either on a computer connected to the analyzer output interface or on a remote monitoring station.

You can use port mirroring on a switch to mirror any of the following:

- **Packets entering or exiting a port**—You can mirror the packets in any combination (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 on an EX2200, EX3200, EX4200, or EX4500 switch**—You can mirror the packets entering a VLAN on these switches to either a local analyzer port or to an analyzer VLAN. On EX3200, EX4200, and EX4500 switches, you can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANS, as ingress input to an analyzer.
- **Packets exiting a VLAN on an EX8200 switch**—You can mirror the packets exiting a VLAN on an EX8200 switch to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANS, as egress input to an analyzer.
- **Statistical samples**—You can mirror a statistical sample of packets that are
 - Entering or exiting a port
 - Entering a VLAN on an EX2200, EX3200, EX4200, or EX4500 switch
 - Exiting a VLAN on an EX8200 switch

You specify the sample number of packets by setting the ratio. You can send the sample to either a local analyzer port or to an analyzer VLAN.

- **Policy-based sample**—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a firewall filter to establish a policy to select the packets to be mirrored. You can send the sample to a local analyzer port or to an analyzer VLAN.



NOTE: Juniper Networks Junos operating system (Junos OS) for EX Series switches implements port mirroring differently than other Junos OS packages. Junos OS for EX Series switches does not include the **port-mirroring** statement found in the **edit forwarding-options** level of the hierarchy of other Junos OS packages, or the **port-mirror** action in firewall filter terms.

Port Mirroring Terminology

Table 1 on page 5 lists some port mirroring terms and their descriptions.

Table 1: Port Mirroring Terminology

Term	Description
Analyzer	<p>A port mirroring configuration on an EX Series switch. The analyzer includes:</p> <ul style="list-style-type: none"> • The name of the analyzer • Source (input) ports or VLAN (optional) • A destination for mirrored packets (either a monitor port or a monitor VLAN) • Ratio field for specifying statistical sampling of packets (optional) • Loss-priority setting
Analyzer output interface (Also known as monitor port)	<p>Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected.</p> <p>NOTE: Interfaces used as output for an analyzer must be configured as family ethernet-switching.</p> <p>Analyzer output interfaces have the following limitations:</p> <ul style="list-style-type: none"> • Cannot also be a source port. • Cannot be used for switching. • Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port mirroring configuration. • Do not retain any VLAN associations they held before they were configured as analyzer output interfaces. <p>If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.</p>
Analyzer VLAN (Also known as monitor VLAN)	<p>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.</p>
Firewall-based analyzer	<p>An analyzer whose configuration does not specify an input source; it specifies only an output destination. A firewall-based analyzer must be used with a firewall filter to achieve the functionality of an analyzer.</p>
Global analyzer (on EX4500 switches only)	<p>An analyzer that is based on a firewall filter, VLAN, or link aggregation group (LAG) or an analyzer in which interfaces are on different port groups on the switch. A port group is a logical group of ports on the switch.</p>
Input interface (Also known as mirrored ports or monitored interfaces)	<p>An interface on the switch that is being mirrored, on traffic that is either entering or exiting the interface. An input interface cannot also be an output interface for an analyzer.</p>
LAG-based analyzer	<p>An analyzer that has a LAG specified as the input (ingress) interface in the analyzer configuration.</p>
Local port mirroring	<p>An analyzer configuration in which packets are mirrored to a local analyzer port.</p>

Table 1: Port Mirroring Terminology (*continued*)

Term	Description
Mirror ratio	See statistical sampling.
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	Mirroring of packets that match the match items in the defined firewall filter term. The action item analyzer analyzer-name is used in the firewall filter to send the packets to the analyzer.
Port-based analyzer	An analyzer session whose configuration defines interfaces for both input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.
Remote port mirroring	<p>Functions the same as local port mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic.</p> <p>If you are using an intermediate (transit) switch, you can avoid flooding of the mirrored traffic to member interfaces of the VLAN by setting the ingress option to specify an interface of the VLAN for ingress-only traffic and the egress option to specify an interface of the VLAN for egress-only traffic in the [edit vlans] hierarchy level. See "Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches" on page 34.</p>
Statistical sampling	<p>You can configure the system to mirror a sampling of the packets by setting a ratio of 1:x, where x is a value from 1 through 2047.</p> <p>For example, when x is set to 1, all packets are copied to the analyzer. When x is set to 200, 1 of every 200 packets is copied.</p>
VLAN-based analyzer	An analyzer session whose configuration uses VLANs for both input and output or for either input or output.

Configuration Guidelines for Port Mirroring on the Switches

When you configure port mirroring, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from the port mirroring feature. Additionally, we recommend that you disable port mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is, select specific interfaces as input to the analyzer) in preference to using the **all** keyword option, which will enable port mirroring on all interfaces. You can also limit the amount of mirrored traffic by using statistical sampling, setting a ratio to select a statistical sample, or using a firewall filter. Mirroring only the necessary packets reduces any potential performance impact.

With local port mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. Thus, while configuring an analyzer, you must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 2 on page 7 summarizes further configuration guidelines for port mirroring on the switches.

Table 2: Configuration Guidelines for Port Mirroring

Guideline	Description	Comment
<p>NOTE: “All other switches” or “All switches” in the Description column applies to switch platforms that support port mirroring. For details on platform support, see EX Series Switch Software Features Overview.</p>		
Number of VLANs that you can use as ingress input to an analyzer	<ul style="list-style-type: none"> 1—EX2200 switches 256—EX3200, EX4200, and EX4500 switches Does not apply—EX8200 switches 	
Number of analyzers that you can enable concurrently	<ul style="list-style-type: none"> 1—EX2200, EX3200, and EX4200 switches 7 port-based or 1 global—EX4500 switches 7 total, with one based on a VLAN, firewall filter, or LAG and with the remaining 6 based on firewall filters—EX8200 switches <p>NOTE: An analyzer configured using a firewall filter does not support mirroring of packets that are egressing ports.</p>	<ul style="list-style-type: none"> You can <i>configure</i> more than the specified number of analyzers on the switch, but you can <i>enable</i> only the specified number for a session. Use disable ethernet-switching-options analyzer name to disable an analyzer. See Table 1 on page 5 for a description of global analyzers. See the next row entry in this table for the exception to the number of firewall-filter-based analyzers allowed on EX4500 switches.
Number of firewall-filter-based analyzers that you can configure on an EX4500 switch	<ul style="list-style-type: none"> 1—EX4500 switches 	If you configure multiple analyzers, you cannot attach any of them to a firewall filter.
Types of ports on which you cannot mirror traffic	<ul style="list-style-type: none"> Virtual Chassis ports (VCPs) Management Ethernet ports (me0 or vme0) Routed VLAN interfaces (RVIs) VLAN-tagged Layer 3 interfaces 	
If port mirroring is configured to mirror packets exiting 10-Gigabit Ethernet ports on EX8200 switches, packets are dropped in both network and mirrored traffic when the mirrored packets exceed 60 percent of the 10-Gigabit Ethernet port traffic.	<ul style="list-style-type: none"> EX8200 switches 	
Traffic directions for which you can specify a ratio	<ul style="list-style-type: none"> Ingress only—EX8200 switches Ingress and egress—All other switches 	
Protocol families that you can include in a firewall-filter-based remote analyzer	<ul style="list-style-type: none"> Any except inet and inet6—EX8200 switches Any—All other switches 	You can use inet and inet6 on EX8200 switches in a local analyzer.

Table 2: Configuration Guidelines for Port Mirroring (*continued*)

Guideline	Description	Comment
Traffic directions that you can configure for mirroring on ports in firewall-filter-based configurations	<ul style="list-style-type: none"> Ingress only—All switches 	
Mirrored packets on tagged interfaces might contain an incorrect VLAN ID or Ethertype.	<ul style="list-style-type: none"> Both VLAN ID and Ethertype—EX2200 switches VLAN ID only—EX3200 and EX4200 switches Ethertype only—EX4500 switches Does not apply—EX8200 switches 	
Mirrored packets exiting an interface do not reflect rewritten class-of-service (CoS) DSCP or 802.1p bits.	<ul style="list-style-type: none"> All switches 	
The analyzer appends an incorrect 802.1Q (dot1q) header to the mirrored packets on the routed traffic or does not mirror any packets on the routed traffic when an egress VLAN that belongs to a routed VLAN interface (RVI) is configured as the input for that analyzer.	<ul style="list-style-type: none"> EX8200 switches Does not apply—All other switches 	As a workaround, configure an analyzer that uses each port (member interface) of the VLAN as egress input.
Packets with physical layer errors are not sent to the local or remote analyzer.	<ul style="list-style-type: none"> All switches 	Packets with these errors are filtered out and thus are not sent to the analyzer.
Port mirroring configuration on a Layer 3 interface with the output configured to a VLAN is not available on EX8200 switches.	<ul style="list-style-type: none"> EX8200 switches Does not apply—All other switches 	
Port mirroring does not support line-rate traffic.	<ul style="list-style-type: none"> All switches 	Port mirroring for line-rate traffic is done on a best-effort basis.

Related Documentation

- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46 or Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Descriptions of Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches](#)

Examples: Port Mirroring Configuration

- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches on page 25](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34](#)

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

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, EX4200, or EX4500 switches
- Packets exiting a VLAN on EX8200 switches

You can analyze the mirrored traffic using a protocol analyzer application installed on a system connected to the local destination interface (or a running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN).

This example describes how to configure an EX Series switch to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on the same switch.

This example describes how to configure local port mirroring:

- [Requirements on page 9](#)
- [Overview and Topology on page 10](#)
- [Mirroring All Employee Traffic for Local Analysis on page 10](#)
- [Mirroring Employee-to-Web Traffic for Local Analysis on page 11](#)
- [Verification on page 13](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch

Before you configure port mirroring, be sure you have an understanding of port mirroring concepts.

Overview and Topology

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to a destination interface on the same switch. 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.

Network Topology

In this example, **ge-0/0/0** and **ge-0/0/1** serve as connections for employee computers.

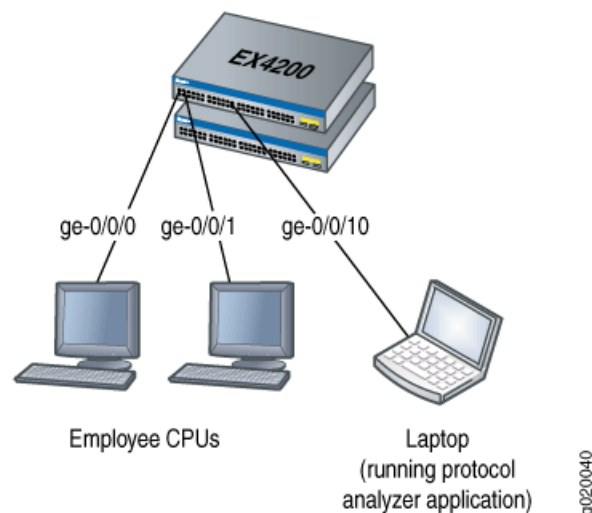
In this example, one interface, **ge-0/0/10**, is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.



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

Figure 1 on page 10 shows the network topology for this example.

Figure 1: Network Topology for Local Port Mirroring Example



Mirroring All Employee Traffic for Local Analysis

To configure port mirroring for all employee traffic for local analysis, perform these tasks:

CLI Quick Configuration

To quickly configure local port mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family inet 192.1.1.1/24
set interfaces ge-0/0/10 unit 0 family ethernet-switching
```

```
set ethernet-switching options analyzer employee-monitor input ingress interface ge-0/0/0.0
set ethernet-switching options analyzer employee-monitor input ingress interface ge-0/0/1.0
set ethernet-switching 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 port-mirror analyzer that we are calling **employee-monitor**:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the output analyzer interface for the **employee-monitor** analyzer. This will be the destination interface for the mirrored packets:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Results Check the results of the configuration:

```
[edit]
user@switch# show
ethernet-switching-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 port mirroring for employee to web traffic, perform these tasks:

CLI Quick Configuration To quickly configure local port mirroring of traffic from the two ports connected to employee computers, filtering so that only traffic to the external Web is mirrored, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options analyzer employee-web-monitor output interface ge-0/0/10.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-web then analyzer
employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure To configure local port 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** analyzer output (the input to the analyzer comes from the action of the filter):

```
[edit ethernet-switching-options]
user@switch# set analyzer 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** analyzer. Accept all traffic to and from the corporate subnet (destination or source address of **192.0.2.16/28**). Send mirrored copies of all packets destined for the Internet (**destination port 80**) to the **employee-web-monitor** analyzer.

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port
80
user@switch# set filter watch-employee term employee-to-web then analyzer
employee-web-monitor
```

4. Apply the **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
ethernet-switching-options {
  analyzer employee-web-monitor {
    output {
      interface ge-0/0/10.0;
    }
  }
}
...
firewall family ethernet-switching {
  filter watch-employee {
    term employee-to-corp {
      from {
```

```

        destination-address 192.0.2.16/28;
        source-address 192.0.2.16/28;
    }
    then accept {
    }
}
term employee-to-web {
    from {
        destination-port 80;
    }
    then analyzer employee-web-monitor;
}
}
}
...
interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                port-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 13](#)

Verifying That the Analyzer Has Been Correctly Created

Purpose Verify that the analyzer named **employee-monitor** or **employee-web-monitor** has been created on the switch with the appropriate input interfaces, and appropriate output interface.

Action You can verify the port mirror analyzer is configured as expected using the **show analyzer** command.

```

user@switch> show analyzer
Analyzer name           : employee-monitor
Output interface        : ge-0/0/10.0
Mirror ratio            : 1
Loss priority           : Low
Ingress monitored interfaces : ge-0/0/0.0

```

Ingress monitored interfaces : ge-0/0/1.0
Egress monitored interfaces : None

Meaning This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, the default setting), a loss priority of low (set this option to high only when the analyzer output is to a VLAN), is mirroring the traffic entering the **ge-0/0/0** and **ge-0/0/1** interfaces, and sending the mirrored traffic to the **ge-0/0/10** interface.

- Related Documentation**
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
 - [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
 - [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
 - [Understanding Port Mirroring on EX Series Switches on page 3](#)

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

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, EX4200, or EX4500 switches
- Packets exiting a VLAN on EX8200 switches

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes 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 port mirroring analyzers when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
 - Using statistical sampling.

- [Setting ratios to select statistical samples.](#)
- [Using firewall filters.](#)

This example describes how to configure remote port mirroring:

- [Requirements on page 15](#)
- [Overview and Topology on page 15](#)
- [Mirroring All Employee Traffic for Remote Analysis on page 16](#)
- [Mirroring Employee-to-Web Traffic for Remote Analysis on page 20](#)
- [Verification on page 24](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- EX Series switch connected to another EX Series switch

Before you configure remote port mirroring, be sure that:

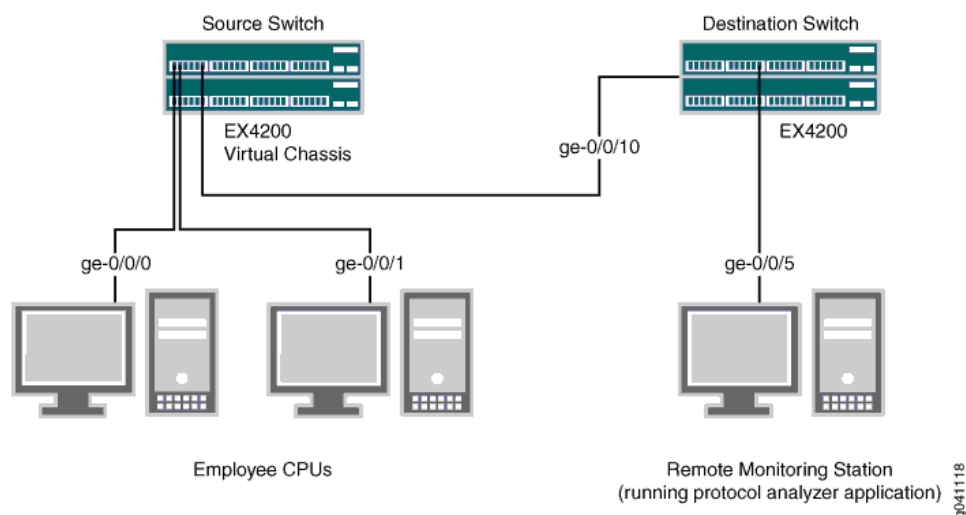
- You have an understanding of port-mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

Overview and Topology

This topic includes two related examples that describe how to configure port 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 2 on page 16](#) shows the network topology for both these example scenarios.

Figure 2: Remote Port Mirroring Example Network 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 the source switch to the destination switch.
- Interface **ge-0/0/5** is a Layer 2 interface that connects the destination switch to the remote monitoring station.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port mirroring 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 port-mode trunk

set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999

set vlans remote-analyzer interface ge-0/0/10 egress

set ethernet-switching-options analyzer employee-monitor input ingress interface ge-0/0/0.0
```



```

set ethernet-switching-options analyzer employee-monitor input ingress interface
ge-0/0/1.0

set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/0.0

set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/1.0

set ethernet-switching-options analyzer employee-monitor loss-priority high

set ethernet-switching-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 port-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 port-mode trunk

set ethernet-switching-options analyzer employee-monitor input ingress vlan
remote-analyzer

set ethernet-switching-options analyzer employee-monitor loss-priority high 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 tag 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 port-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999

```

- Configure the **ge-0/0/10** interface for egress-only traffic so that traffic can only egress from the interface:

```

[edit vlans]
user@switch# set remote-analyzer interface ge-0/0/10 egress

```

- Configure the **employee-monitor** analyzer:

```

[edit ethernet-switching-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 loss-priority high

```

```
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. On the destination switch:

- Configure the VLAN tag 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 port-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 port-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/5.0
```

Results Check the results of the configuration on the source switch:

```
[edit]
user@switch# show
ethernet-switching-options {
  analyzer employee-monitor {
    loss-priority high;
    input {
      ingress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
      egress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
    }
  }
  output {
    vlan {
      remote-analyzer;
    }
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
```

```

        port-mode trunk;
        vlan {
            members 999;
        }
    }
}
vpls {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            egress;
        }
    }
}
}

```

Check the results of the configuration on the destination switch:

```

[edit]
user@switch# show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vpls {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            egress;
        }
    }
}
}
ethernet-switching-options {
    analyzer employee-monitor {
        loss-priority high;
        input {

```

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

Mirroring Employee-to-Web Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis of employee to web traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port mirroring to mirror employee traffic to the external Web, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch terminal window:

[edit]

```
set ethernet-switching-options analyzer employee-web-monitor loss-priority high output
vlan 999
```

```
set vlans remote-analyzer vlan-id 999
```

```
set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
```

```
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-corp
from destination-address 192.0.2.16/28
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-corp
from source-address 192.0.2.16/28
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-corp
then accept
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-web
from destination-port 80
```

```
set firewall family ethernet-switching filter watch-employee term employee-to-web
then analyzer employee-web-monitor
```

```
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
```

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

- Copy and paste the following commands in the destination switch terminal window:

[edit]

```
set vlans remote-analyzer vlan-id 999
```

```
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-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 port-mode trunk

set ethernet-switching-options analyzer employee-web-monitor input ingress vlan
remote-analyzer

set ethernet-switching-options analyzer employee-web-monitor loss-priority high output
interface ge-0/0/5.0

```

Step-by-Step Procedure To configure port mirroring of all traffic from the two ports connected to employee computers to the **remote-analyzer** VLAN for use from a remote monitoring station:

1. On the source switch:

- Configure the **employee-web-monitor** analyzer:

```

[edit ethernet-switching-options]
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode
trunk
user@switch# set analyzer employee-web-monitor loss-priority high output vlan 999

```

- Configure the VLAN tag 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 192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port
80
user@switch# set filter watch-employee term employee-to-web then analyzer
employee-web-monitor

```

- 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 tag 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 port-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 port-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-web-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-web-monitor loss-priority high 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 {
        port-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 {
            192.0.2.16/28;
        }
        destination-address {
            192.0.2.16/28;
        }
    }
    then accept;
}
term employee-to-web {
    from {
        destination-port 80;
    }
    then analyzer employee-web-monitor;
}
}
}
ethernet-switching-options {
    analyzer employee-web-monitor {
        loss-priority high;
        output {
            vlan {
                999;
            }
        }
    }
}
vllans {
    remote-analyzer {
        vlan-id 999;
    }
}
}

```

Check the results of the configuration on the destination switch:

```

[edit]
user@switch# show
vllans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
}
ge-0/0/5 {
    unit 0 {
        family ethernet-switching {

```

```
        port-mode trunk;
    }
}
}
ethernet-switching-options {
    analyzer employee-web-monitor {
        loss-priority high;
        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 24](#)

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 | <p>You can verify 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.</p> <p>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:</p> <pre>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</pre> |
| Meaning | This output shows that the employee-monitor analyzer has a ratio of 1 (mirroring every packet, the default), has a loss priority of high (set this option to high whenever the analyzer output is to a VLAN), is mirroring the traffic entering ge-0/0/0 and ge-0/0/1 , and is sending the mirrored traffic to the analyzer called remote-analyzer . |
| Related Documentation | <ul style="list-style-type: none">• Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9 |

- [Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches on page 25](#)
- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)

Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches

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, EX4200, or EX4500 switches
- Packets exiting a VLAN on EX8200 switches



NOTE: The feature of mirroring traffic to multiple VLAN interfaces is available only on EX8200 switches.

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This example describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN so that you can perform analysis from a remote monitoring station. The **remote-analyzer** VLAN in this example contains multiple member interfaces. Therefore, the same traffic is mirrored to all member interfaces of the **remote-analyzer** VLAN so that mirrored packets can be sent to different remote monitoring stations. You can install applications, such as sniffers and intrusion detection systems, on remote monitoring stations to analyze these mirrored packets and to obtain useful statistical data. For instance, if there are two remote monitoring stations, you can install a sniffer on one remote monitoring station and an intrusion detection system on the other station. You can use a firewall filter analyzer configuration to forward a specific type of traffic to a remote monitoring station.



BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured port mirroring analyzers when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:

- Using statistical sampling.
- Setting ratios to select statistical samples.
- Using firewall filters.

This example describes how to configure remote port mirroring to multiple interfaces on an analyzer VLAN:

- [Requirements on page 26](#)
- [Overview and Topology on page 26](#)
- [Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis on page 28](#)
- [Verification on page 33](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- Three EX8200 switches

Before you configure remote port mirroring, be sure that:

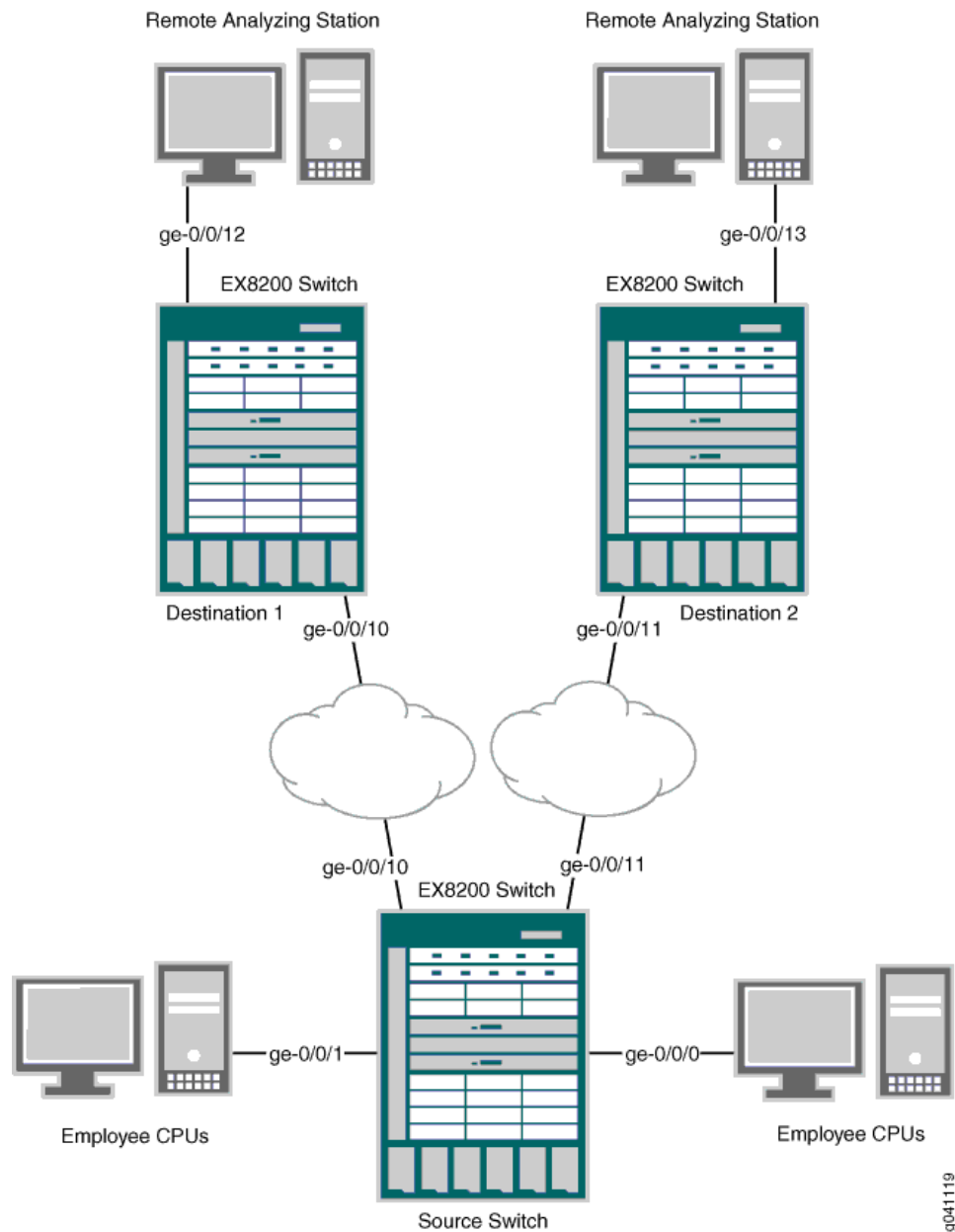
- You have an understanding of port-mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

Overview and Topology

This example describes how to configure port mirroring to multiple interfaces in the **remote-analyzer** VLAN so that traffic is sent to different remote monitoring stations for analysis.

[Figure 3 on page 27](#) shows the network topology for this example.

Figure 3: Remote Port Mirroring Example Network Topology Using Multiple VLAN Member Interfaces



g041119

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.
- Interfaces **ge-0/0/10** and **ge-0/0/11** are Layer 2 interfaces that are connected to different destination switches.

- Interface **ge-0/0/12** is a Layer 2 interface that connects the Destination 1 switch to the remote monitoring station.
- Interface **ge-0/0/13** is a Layer 2 interface that connects the Destination 2 switch to the remote monitoring station.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis

To configure port mirroring to multiple VLAN member interfaces for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port mirroring for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- In the source switch terminal window, copy and paste the following commands:
[edit]

set vlans remote-analyzer vlan-id 999

set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999

set vlans remote-analyzer interface ge-0/0/10 egress

set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 999

set vlans remote-analyzer interface ge-0/0/11 egress

set ethernet-switching-options analyzer employee-monitor input ingress interface ge-0/0/0.0

set ethernet-switching-options analyzer employee-monitor input ingress interface ge-0/0/1.0

set ethernet-switching-options analyzer employee-monitor input egress interface ge-0/0/0.0

set ethernet-switching-options analyzer employee-monitor input egress interface ge-0/0/1.0

set ethernet-switching-options analyzer employee-monitor loss-priority high

set ethernet-switching-options analyzer employee-monitor output vlan remote-analyzer
- In the Destination 1 switch terminal window, copy and paste the following commands:
[edit]

set vlans remote-analyzer vlan-id 999

set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk

set vlans remote-analyzer interface ge-0/0/10 ingress

```

set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode trunk

set ethernet-switching-options analyzer employee-monitor input ingress vlan
remote-analyzer

set ethernet-switching-options analyzer employee-monitor loss-priority high output
interface ge-0/0/12.0

```

- In the Destination 2 switch terminal window, copy and paste the following commands:

```

[edit]

set vlans remote-analyzer vlan-id 999

set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk

set vlans remote-analyzer interface ge-0/0/11 ingress

set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode trunk

set ethernet-switching-options analyzer employee-monitor input ingress vlan
remote-analyzer

set ethernet-switching-options analyzer employee-monitor loss-priority high output
interface ge-0/0/13.0

```

Step-by-Step Procedure

To configure basic remote port mirroring to two VLAN member interfaces:

1. On the source switch:

- Configure the VLAN tag ID for the **remote-analyzer** VLAN:

```

[edit vlans]
user@switch# set remote-analyzer vlan-id 999

```

- Configure the interfaces on the network port connected to destination switches for trunk mode and associate it with the **remote-analyzer** VLAN:

```

[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/11 unit 0 family ethernet-switching vlan members 999

```

- Configure **ge-0/0/10** and **ge-0/0/11** for egress-only traffic so that traffic can only exit from the interface:

```

[edit vlans]
user@switch# set remote-analyzer interface ge-0/0/10 egress
user@switch# set remote-analyzer interface ge-0/0/11 egress

```

- Configure the **employee-monitor** analyzer:

```

[edit ethernet-switching-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 loss-priority high
user@switch# set analyzer employee-monitor output vlan remote-analyzer

```

2. On the Destination 1 switch:

- Configure the VLAN tag ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the **ge-0/0/10** interface on the Destination 1 switch for trunk mode, associate it with the **remote-analyzer** VLAN, and set the interface for ingress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/10 ingress
```

- Configure the interface connected to the remote monitoring station for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching port-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/12.0
```

3. On the Destination 2 switch:

- Configure the VLAN tag ID for the **remote-analyzer** VLAN:

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure the **ge-0/0/11** interface on the Destination 2 switch for trunk mode, associate it with the **remote-analyzer** VLAN, and set the interface only for ingress traffic:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/11 ingress
```

- Configure the interface connected to the remote monitoring station for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/13.0
```

Results Check the results of the configuration on the source switch:

```
[edit]
user@switch# show
ethernet-switching-options {
  analyzer employee-monitor {
    loss-priority high;
    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;
    }
  }
}
vpls {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/10.0 {
        egress;
      }
      ge-0/0/11.0 {
        egress;
      }
    }
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 999;
        }
      }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          member 999;
        }
      }
    }
  }
}
```

```
}
```

Check the results of the configuration on the Destination 1 switch:

```
[edit]
user@switch# show
vpls {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/10.0 {
        ingress;
      }
    }
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      ethernet-switching {
        port-mode trunk;
      }
    }
  }
  ge-0/0/12 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
      }
    }
  }
}
ethernet-switching-options {
  analyzer employee-monitor {
    loss-priority high;
    input {
      ingress {
        vlan remote-analyzer;
      }
    }
    output {
      interface {
        ge-0/0/12.0;
      }
    }
  }
}
```

Check the results of the configuration on the Destination 2 switch:

```
[edit]
user@switch# show
vpls {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/11.0 {
```



```

        ingress;
    }
}
}
interfaces {
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
            }
        }
    }
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
            }
        }
    }
}
ethernet-switching-options {
    employee-monitor {
        loss-priority high;
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/13.0;
            }
        }
    }
}
}

```

Verification

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

- [Verifying That the Analyzer Has Been Correctly Created on page 33](#)

Verifying That the Analyzer Has Been Correctly Created

Purpose Verify that the analyzer named **employee-monitor** has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action You can verify the analyzer is configured as expected by using the **show 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 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
```

Meaning This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, the default), has a loss priority of high (set this option to high whenever the analyzer output is to a VLAN), is mirroring the traffic entering **ge-0/0/0** and **ge-0/0/1**, and is sending the mirrored traffic to the analyzer called **remote-analyzer**.

**Related
Documentation**

- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)

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

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, EX4200, or EX4500 switches
- Packets exiting a VLAN on EX8200 switches

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes an example that describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN through a transit switch, so that you can perform analysis from a remote monitoring station.



BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured port mirroring analyzers when you are not using them.

- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
 - Using statistical sampling.
 - Setting ratios to select statistical samples.
 - Using firewall filters.

This example describes how to configure remote port mirroring through a transit switch:

- [Requirements on page 35](#)
- [Overview and Topology on page 35](#)
- [Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch on page 36](#)
- [Verification on page 41](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- EX3200 or EX4200 switch connected to another EX3200 or EX4200 switch through a third EX3200 or EX4200 switch

Before you configure remote port mirroring, be sure that:

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

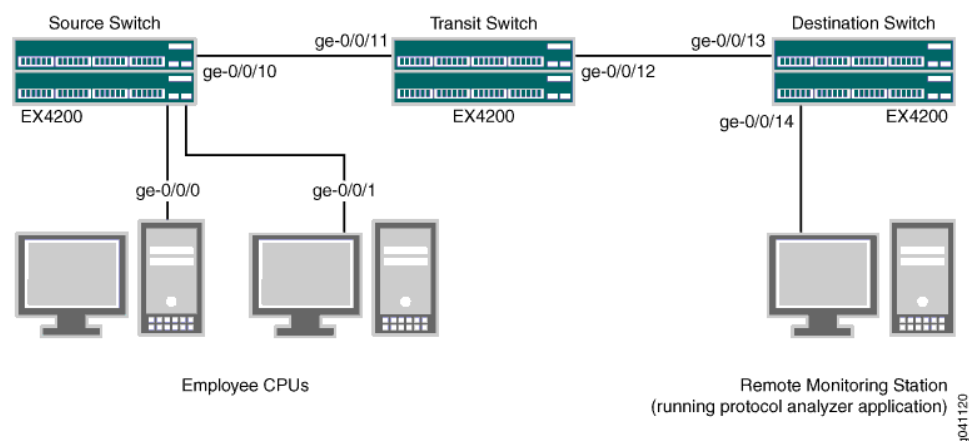
Overview and Topology

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 36](#) shows the network topology for this example.

Figure 4: Remote Port Mirroring Example Through a Transit Switch Network 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 port 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 port 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 port-mode trunk
```

```
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

```
set ethernet-switching-options analyzer employee-monitor input ingress interface
ge-0/0/0.0
```

```
set ethernet-switching-options analyzer employee-monitor input ingress interface
ge-0/0/1.0
```

```
set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/0.0
```

```
set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/1.0
```

```
set ethernet-switching-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 port-mode trunk
```

```
set vlans remote-analyzer interface ge-0/0/11 ingress
```

```
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode trunk
```

```
set vlans remote-analyzer interface ge-0/0/12 egress
```

```
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 port-mode trunk
```

```
set vlans remote-analyzer interface ge-0/0/13 ingress
```

```
set interfaces ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
```

```
set ethernet-switching-options analyzer employee-monitor input ingress vlan
remote-analyzer
```

```
set ethernet-switching-options analyzer employee-monitor loss-priority high output
interface ge-0/0/14.0
```

Step-by-Step Procedure

To configure remote port mirroring through a transit switch:

1. On the source switch:

- Configure the VLAN tag 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 port-mode trunk
```

```
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-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 loss-priority high
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. On the transit switch:

- Configure the VLAN tag 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, and set the interface for ingress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/11 ingress
```

- 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 port-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/12 egress
```

- 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 tag 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 port-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

- Configure the interface connected to the remote monitoring station for trunk mode:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
```

- Configure the **employee-monitor** analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/14.0
```

Results Check the results of the configuration on the source switch:

```
[edit]
user@switch# show
ethernet-switching-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;
      }
    }
  }
}
vlangs {
  remote-analyzer {
    vlan-id 999;
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          member 999;
        }
      }
    }
  }
}
}
```

Check the results of the configuration on the transit switch:

```
[edit]
user@switch# show
vlangs {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/11.0 {
```

```
        ingress;
      }
      ge-0/0/12.0 {
        egress;
      }
    }
    no-mac-learning;
  }
}
interfaces {
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
      }
    }
  }
  ge-0/0/12 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
      }
    }
  }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch# show
vpls {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/13.0 {
        ingress;
      }
    }
  }
}
interfaces {
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
      }
    }
  }
  ge-0/0/14 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
      }
    }
  }
}
```



```

ethernet-switching-options {
  analyzer employee-monitor {
    loss-priority high;
    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 41](#)

Verifying That the Analyzer Has Been Correctly Created

Purpose Verify that the analyzer named **employee-monitor** has been created on the switch with the appropriate input interfaces and the appropriate output interface.

Action You can verify the analyzer is configured as expected by using the **show 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 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

```

Meaning This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, the default), has a loss priority of high (set this option to high whenever the analyzer output is to a VLAN), is mirroring the traffic entering **ge-0/0/0** and **ge-0/0/1**, and is sending the mirrored traffic to the analyzer called **remote-analyzer**.

- Related Documentation**
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
 - [Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches on page 25](#)

- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)

Configuring Port Mirroring

- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)

Configuring Port Mirroring to Analyze Traffic (CLI Procedure)

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, EX4200, or EX4500 switches
- Packets exiting a VLAN on EX8200 switches



BEST PRACTICE: Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured port mirroring analyzers when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
 - Using statistical sampling.
 - Setting ratios to select statistical samples.
 - Using firewall filters.



NOTE: If you want to create additional analyzers without deleting the existing analyzer, first disable the existing analyzer using the `disable analyzer analyzer-name` command or the J-Web configuration page for port mirroring.



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

- [Configuring Port Mirroring for Local Traffic Analysis on page 43](#)
- [Configuring Port Mirroring for Remote Traffic Analysis on page 43](#)
- [Filtering the Traffic Entering an Analyzer on page 44](#)

Configuring Port Mirroring for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch:

1. Choose a name for the analyzer—in this case, **employee-monitor**—and specify the input—in this case, packets entering **ge-0/0/0** and **ge-0/0/1**:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
```

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

When the ratio is set to 200, 1 of every 200 packets is mirrored to the analyzer. You can use statistical sampling to reduce the volume of mirrored traffic, as a high volume of mirrored traffic can be performance intensive for the switch. On EX8200 switches, you can set a ratio only for ingress packets.

3. Configure the destination interface for the mirrored packets:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuring Port Mirroring for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location:

1. Configure a VLAN to carry the mirrored traffic. This VLAN is called **remote-analyzer** and given the ID of 999 by convention in this documentation:

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Set the uplink module interface that is connected to the distribution switch to trunk mode and associate it with the **remote-analyzer** VLAN:

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching port-mode trunk
vlan members 999
```

3. Configure the analyzer:

- a. Choose a name and set the loss priority to high. Loss priority should always be set to high when configuring for remote port mirroring:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor loss-priority high
```

- b. Specify the traffic to be mirrored—in this example the packets entering ports **ge-0/0/0** and **ge-0/0/1**:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0

[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

- c. Specify the **remote-analyzer** VLAN as the output for the analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

When the ratio is set to 200, 1 out of every 200 packets is mirrored to the analyzer. You can use this to reduce the volume of mirrored traffic as a very high volume of mirrored traffic can be performance intensive for the switch.

Filtering the Traffic Entering an Analyzer

To filter which packets are mirrored to an analyzer, create the analyzer and then use it as the action in the firewall filter. You can use firewall filters in both local and remote port mirroring configurations.

If the same analyzer is used in multiple filters or terms, the packets are copied to the analyzer output port or analyzer VLAN only once.

To filter mirrored traffic, create an analyzer and then create a firewall filter. The filter can use any of the available match conditions and must have an action of **analyzer analyzer-name**. The action of the firewall filter provides the input to the analyzer.

To configure port mirroring with filters:

1. Configure the analyzer name (here, **employee-monitor**) and the output:

- a. For local analysis, set the output to the local interface to which you will connect the computer running the protocol analyzer application:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

- b. For remote analysis, set the loss priority to high and set the output to the **remote-analyzer** VLAN:

```
[edit ethernet-switching-options]
```

```
user@switch# set analyzer employee-monitor loss-priority high output vlan 999
```

2. Create a firewall filter using any of the available match conditions and specify the action as **analyzer employee-monitor**:

This step shows a firewall filter called **example-filter**, with two terms:

- a. Create the first term to define the traffic that should not pass through to the analyzer:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from source-address ip-address
```

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from destination-address
ip-address
```

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer then accept
```

- b. Create the second term to define the traffic that should pass through to the analyzer:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
```

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then analyzer employee-monitor
```

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then accept
```

3. Apply the firewall filter to the interfaces or VLAN that are input to the analyzer:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input
example-filter
```

```
[edit]
user@switch# set vlan remote-analyzer filter input example-filter
```

Related Documentation

- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)
- [Firewall Filters for EX Series Switches Overview](#)

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

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, EX4200, or EX4500 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 first part of the screen displays analyzer details such as the name, status, analyzer port, ratio, and loss priority.

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



NOTE: After you make changes to the configuration in 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:

- Add—Add an analyzer. Enter information as specified in [Table 3 on page 47](#).
- Edit—Modify details of the selected analyzer. Enter information as specified in [Table 3 on page 47](#).
- 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.



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

Table 3: Port Mirroring Configuration Settings

Field	Function	Your Action
Analyzer Name	Specifies the name of the analyzer.	Type a name for the analyzer.
Ratio	Specifies the ratio of packets to be mirrored. For example: <ul style="list-style-type: none"> A ratio of 1 sends copies of all packets. A ratio of 2047 sends copies of 1 out of every 2047 packets. 	Enter a number from 0 through 2047.
Loss Priority	Specifies the loss priority of the mirrored packets. 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. 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. 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.
Ingress	Specifies interfaces or VLANs for which entering traffic is mirrored.	Click Add and select Port or VLAN. Next, select the interfaces or VLANs. Click Remove to delete an ingress interface or VLAN.
Egress	Specifies interfaces for which exiting traffic is mirrored.	Click Add to add egress interfaces. Click Remove to remove egress interfaces.

- Related Documentation**
- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
 - [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
 - [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
 - [Understanding Port Mirroring on EX Series Switches on page 3](#)

Verifying Port Mirroring Configuration

- [Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches on page 47](#)

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.

Related Documentation

- [Configuring Port Mirroring to Analyze Traffic \(J-Web Procedure\) on page 46](#)
- [Configuring Port Mirroring to Analyze Traffic \(CLI Procedure\) on page 42](#)
- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)

Configuration Statements for Port Mirroring

- [\[edit ethernet-switching-options\] Configuration Statement Hierarchy on page 49](#)

[edit ethernet-switching-options] Configuration Statement Hierarchy

```

ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
    }
    output {
      interface interface-name;
      vlan (vlan-id | vlan-name) {
        no-tag;
      }
    }
  }
}
bpdu-block {
  disable-timeout timeout;
  interface (all | [interface-name]);
}
dot1q-tunneling {
  ether-type (0x8100 | 0x88a8 | 0x9100);
}
interfaces interface-name {
  no-mac-learning;
}
mac-notification {
  notification-interval seconds;
}
mac-table-aging-time seconds;
nonstop-bridging;
port-error-disable {
  disable-timeout timeout;
}
redundant-trunk-group {
  group name {
    preempt-cutover-timer seconds;
    interface
      primary;
    }
    interface
  }
}
secure-access-port {
  dhcp-snooping-file {
    location local_pathname | remote_URL;
  }
}

```

```
    timeout seconds;
    write-interval seconds;
  }
  interface (all | interface-name) {
    allowed-mac {
      mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted );
    fcoe-trusted;
    mac-limit limit action action;
    no-allowed-mac-log;
    static-ip ip-address {
      vlan vlan-name;
      mac mac-address;
    }
  }
}
vlan (all | vlan-name) {
  (arp-inspection | no-arp-inspection) [
    forwarding-class class-name;
  ]
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix hostname | mac | none;
      use-interface-description;
      use-string string;
    }
    vendor-id [string];
  }
  (examine-dhcp | no-examine-dhcp) {
    forwarding-class class-name;
  }
  examine-fip {
    fc-map fc-map-value;
  }
  (ip-source-guard | no-ip-source-guard);
  mac-move-limit limit action action;
}
}
static {
  vlan name {
    mac mac-address {
      next-hop interface-name;
    }
  }
}
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    no-broadcast;
    no-multicast;
```

```

        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
    flag flag <disable>;
}
unknown-unicast-forwarding {
    vlan (all | vlan-name) {
        interface interface-name;
    }
}
voip {
    interface (all | [interface-name | access-ports]) {
        vlan vlan-name ;
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
            network-control);
    }
}
}

```

Related Documentation

- [Understanding Port Mirroring on EX Series Switches on page 3](#)
- Port Security for EX Series Switches Overview
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding Storm Control on EX Series Switches
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding Q-in-Q Tunneling on EX Series Switches
- Understanding Unknown Unicast Forwarding on EX Series Switches
- Understanding MAC Notification on EX Series Switches
- Understanding FIP Snooping
- Understanding Nonstop Bridging on EX Series Switches

analyzer

Syntax

```
analyzer {  
  name {  
    ratio number;  
    loss-priority priority;  
    input {  
      ingress {  
        interface (all | interface-name);  
        vlan (vlan-id | vlan-name);  
      }  
      egress {  
        interface (all | interface-name);  
      }  
    }  
    output {  
      interface interface-name;  
      vlan (vlan-id | vlan-name) {  
        no-tag;  
      }  
    }  
  }  
}
```

Hierarchy Level [edit [ethernet-switching-options](#)]

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

Description Configure port mirroring. One analyzer (port mirroring configuration) can be configured on an EX2200, EX3200, EX4200, or EX4500 switch and seven analyzers (port mirroring configurations) can be configured on an EX8208 or EX8216 switch at a time. Other analyzers can be present and disabled.

Default Port mirroring is disabled and Junos OS creates no default analyzers.

Options *name*—Name that identifies the analyzer. The name can be up to 125 characters long, must begin with a letter, and can include uppercase letters, lowercase letters, numbers, dashes, and underscores. No other special characters are allowed.

The remaining statements are explained separately.

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

Related Documentation

- [Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14](#)
- [Understanding Port Mirroring on EX Series Switches on page 3](#)

egress

Syntax	<code>egress;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> vlan-id <i>number</i> interface <i>interface-name</i>]</code>
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	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34

egress (Interface or VLAN)

Syntax	<pre>egress { interface (all <i>interface-name</i>); vlan (<i>vlan-id</i> <i>vlan-name</i>); }</pre>
Hierarchy Level	<code>[edit ethernet-switching-options analyzer name input]</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Specify ports or VLANs for which traffic exiting the interface or VLAN is mirrored in a port mirroring configuration. You can define the egress VLAN ID or VLAN name for port mirroring only for EX8200 switches.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34

ethernet-switching-options

```
Syntax ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
        }
      }
    }
    output {
      interface interface-name;
      vlan (vlan-id | vlan-name) {
        no-tag;
      }
    }
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]);
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-notification {
    notification-interval seconds;
  }
  mac-table-aging-time seconds;
  nonstop-bridging;
  port-error-disable {
    disable-timeout timeout;
  }
  redundant-trunk-group {
    group name {
      interface interface-name <primary>;
      interface interface-name;
    }
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
  }
}
```

```

interface (all | interface-name) {
    allowed-mac {
        mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action action;
    no-allowed-mac-log;
    static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
    }
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
        forwarding-class class-name;
    ]
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
        vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit limit action action;
}
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}

```

```
}
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable |
    no-world-readable>;
  flag flag <disable>;
}
unknown-unicast-forwarding {
  vlan (all | vlan-name) {
    interface interface-name;
  }
}
voip {
  interface (all | [interface-name | access-ports]) {
    vlan vlan-name ;
    forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
      network-control);
  }
}
}
```

Hierarchy Level [edit]

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

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation

- [Understanding Port Mirroring on EX Series Switches on page 3](#)
- Port Security for EX Series Switches Overview
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding Storm Control on EX Series Switches
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding Q-in-Q Tunneling on EX Series Switches
- Understanding Unknown Unicast Forwarding on EX Series Switches
- Understanding MAC Notification on EX Series Switches
- Understanding FIP Snooping
- Understanding Nonstop Bridging on EX Series Switches

ingress

Syntax	<code>ingress;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> vlan-id <i>number</i> interface <i>interface-name</i>]</code>
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	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34

ingress (Interface or VLAN)

Syntax	<pre>ingress { interface (all <i>interface-name</i>); vlan (<i>vlan-id</i> <i>vlan-name</i>); }</pre>
Hierarchy Level	<code>[edit ethernet-switching-options analyzer name input]</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure ports or VLANs for which the entering traffic is mirrored as part of a port mirroring configuration. You can define the ingress VLAN ID or VLAN name for port mirroring for all switches except EX8200 switches.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34

input

Syntax	<pre>input { ingress { interface (all <i>interface-name</i>); vlan (<i>vlan-id</i> <i>vlan-name</i>); } egress { interface (all <i>interface-name</i>); } }</pre>
Hierarchy Level	[edit ethernet-switching-options analyzer name]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Define the traffic to be mirrored in a port mirroring configuration—the definition can be a combination of:</p> <ul style="list-style-type: none">• Packets entering or exiting a port• Packets entering a VLAN on an EX2200, EX3200, EX4200, or EX4500 switch• Packets exiting a VLAN on an EX8200 switch <p>The remaining statements are explained separately.</p>
Default	No default.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9• Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14• Understanding Port Mirroring on EX Series Switches on page 3

interface

Syntax	interface (all <i>interface-name</i>);
Hierarchy Level	[edit ethernet-switching-options analyzer name input egress], [edit ethernet-switching-options analyzer name input ingress], [edit ethernet-switching-options analyzer name output]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the interfaces for which traffic is mirrored.
Options	<p>all—Apply port mirroring to all interfaces on the switch. Mirroring a high volume of traffic can be performance intensive for the switch. 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.</p> <p><i>interface-name</i>—Apply port mirroring to the specified interface only.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9 • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14 • Understanding Port Mirroring on EX Series Switches on page 3

loss-priority

Syntax	<code>loss-priority <i>priority</i>;</code>
Hierarchy Level	[edit ethernet-switching-options analyzer name]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a loss priority for mirrored packets. By default, the switch applies a lower priority to mirrored data than to regular port-to-port data—mirrored traffic is dropped in preference for regular traffic when capacity is exceeded. For port mirroring configurations with output to an analyzer VLAN, set the loss priority to high.
Default	Low
Options	<i>priority</i> —The value for priority can be low or high. Default: low
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Port Mirroring on EX Series Switches on page 3• Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14

no-tag

Syntax	<code>no-tag;</code>
Hierarchy Level	[edit ethernet-switching-options analyzer name output vlan (vlan-id vlan-name)]
Release Information	Statement introduced in Junos OS Release 11.3 for EX Series switches.
Description	Specify that remote port mirroring packets are not tagged.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX Series Switches on page 25• Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9• Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14

output

Syntax	<pre>output { interface interface-name; vlan (vlan-id vlan-name) { no-tag; } }</pre>
Hierarchy Level	[edit ethernet-switching-options analyzer name]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure the destination for mirrored traffic, either an interface on the switch, for local monitoring, or a VLAN, for remote monitoring. You can optionally configure the no-tag statement so that remote port mirroring packets are not tagged.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches on page 9 • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14

ratio

Syntax	<i>ratio number;</i>
Hierarchy Level	[edit ethernet-switching-options analyzer name]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure port mirroring to copy a sampling of packets, by setting a ratio of 1:x. A value of 1 for x mirrors every packet, and 2047 mirrors 1 out of every 2047 packets.</p> <p>On EX8200 switches, you can set a ratio only for ingress packets.</p> <p>On EX4500 switches, if you configure a ratio for any one of the port-based analyzers, that ratio automatically applies to all port-based analyzers.</p>
Default	1
Options	<p><i>number</i>—The number of packets in the sample, out of which 1 packet is mirrored.</p> <p>Range: 1 through 2047</p> <p>Default: 1</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Port Mirroring on EX Series Switches on page 3

vlan

Syntax	<code>vlan (vlan-id vlan-name) { no-tag; }</code>
Hierarchy Level	[edit ethernet-switching-options analyzer name input egress], [edit ethernet-switching-options analyzer name input ingress], [edit ethernet-switching-options analyzer name output]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure mirrored traffic to be sent to a VLAN for remote monitoring. On a destination (output) VLAN, you can also configure the no-tag statement.
Options	<i>vlan-id</i> —Numeric VLAN identifier. <i>vlan-name</i> —Name of the VLAN. The remaining statement is explained separately.
Required Privilege Level	<i>system</i> —To view this statement in the configuration. <i>routing-control</i> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches on page 34 • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches on page 14

Operational Commands for Port Mirroring

show analyzer

Syntax	show analyzer <i>analyzer-name</i>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display information about analyzers configured for port mirroring.
Options	<i>analyzer-name</i> —(Optional) Displays the status of a specific analyzer on the switch.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Understanding Port Mirroring on EX Series Switches on page 3
List of Sample Output	show analyzer on page 64
Output Fields	Table 4 on page 64 lists the output fields for the command-name command. Output fields are listed in the approximate order in which they appear.

Table 4: 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, between 1 and 2047 where 1 sends copies of all packets and 2047 sends copies of 1 out of every 2047 packets.
Loss priority	Displays the loss priority of mirrored packets. By default, loss priority is set to low , with mirrored traffic dropped in preference for regular traffic when capacity is exceeded. For analyzers with output to a VLAN, set the loss priority to high .
Egress monitored interfaces	Displays interfaces for which traffic exiting the interfaces is mirrored.
Ingress monitored interfaces	Displays interfaces for which traffic entering the interfaces is mirrored.
Ingress monitored VLANs	Displays VLANs for which traffic entering the VLAN is mirrored.

Sample Output

```

show analyzer user@host> show analyzer
Analyzer name      : employee-monitor
Output interface   : ge-0/0/10.0
Output VLAN        : remote-analyzer

```



```
Mirror ratio           : 1
Loss priority          : High
Egress monitored interfaces : ge-0/0/3.0
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
```


CHAPTER 2

sFlow Monitoring Technology

- [sFlow Technology—Overview on page 67](#)
- [Example: sFlow Technology Configuration on page 70](#)
- [Configuring sFlow Technology on page 74](#)
- [Configuration Statements for sFlow Technology on page 76](#)
- [Operational Commands for sFlow Technology on page 89](#)

sFlow Technology—Overview

- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)

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 67](#)
- [Adaptive Sampling on page 68](#)
- [sFlow Agent Address Assignment on page 69](#)

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* (see <http://faqs.org/rfcs/rfc3176.html>).



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. It 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 messages to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Because sampling is distributed across subagents, the protocol overhead associated with sFlow technology is significantly reduced at the collector.



NOTE: 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 their sampling rate to the 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 5 seconds the agent checks interfaces to get the number of samples, and interfaces are grouped based on the slot that they belong to. The top five interfaces that produce the highest number of samples are selected. Using the binary backoff algorithm, the sampling load on these interfaces is reduced by half and allotted to interfaces that have a lower sampling rate. Therefore when the processor

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 are not reported in the sFlow information, but over time the majority of flows are reported. Based on a defined sampling rate, 1 out of N packets is captured and sent to the collector. This type of sampling does not provide a 100 percent accurate result in the analysis, but it does provide a result with quantifiable accuracy. A user-configured polling interval defines how often 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 for the sFlow agent remains constant. If you do not specify the IP address to be assigned to the agent, an IP address is automatically assigned to the agent based on the following order of priority of interfaces configured on the switch:

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 routed VLAN interface (RVI) is used as the source IP address.

Related Documentation

- [Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70](#)
- [Configuring sFlow Technology for Network Monitoring \(CLI Procedure\) on page 74](#)
- [Monitoring Interface Status and Traffic](#)

Example: sFlow Technology Configuration

- [Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70](#)

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

You can configure sFlow technology, designed for monitoring high-speed switched or routed networks, to continuously monitor traffic at wire speed on all interfaces simultaneously. You can specify sample rates for ingress and egress packets. sFlow data can be used to provide network traffic visibility information.

This example describes how to configure and use sFlow technology to monitor network traffic. Junos OS fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks* (see <http://faqs.org/rfcs/rfc3176.html>).

- [Requirements on page 70](#)
- [Overview and Topology on page 70](#)
- [Configuration on page 71](#)
- [Verification on page 73](#)

Requirements

This example uses the following hardware and software components:

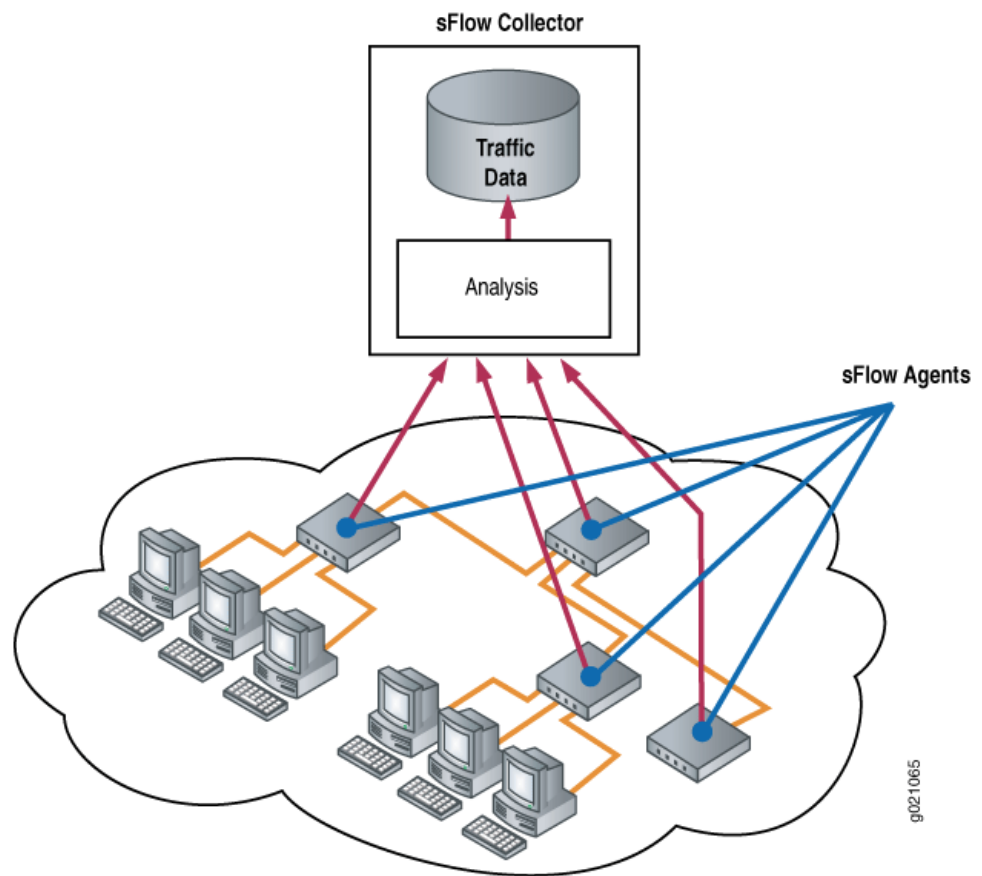
- One EX Series switch
- Junos OS Release 9.3 or later for EX Series switches

Overview and Topology

sFlow technology is a statistical-sampling-based network monitoring technology for high-speed switched or routed networks. sFlow technology samples network packets and sends the samples to a monitoring station. You can specify sample 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 71](#) depicts the basic elements of the sFlow system.

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
```

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.

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—that is, an aggregated Ethernet interface with a name such as ae0. You can enable sFlow technology on the member interfaces that make up the LAG.

3. Specify 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:



NOTE: The sample-rate *number* (the global sample-rate) statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.

```
[edit protocols sflow]
user@switch# set sample-rate egress 1000
```



NOTE: If you set only the egress sample rate, the ingress sample rate will be disabled.

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 Has Been Configured Properly on page 73](#)
- [Verifying That sFlow Technology Is Enabled on the Intended Interface on page 73](#)
- [Verifying the sFlow Collector Configuration on page 74](#)

Verifying That sFlow Technology Has Been Configured Properly

Purpose Verify that sFlow technology has been 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 sample limit cannot be configured and is set to 300 packets/second.

Meaning The output shows that sFlow technology is enabled and specifies the values for the sample limit, polling interval, and sample rate.

Verifying That sFlow Technology Is Enabled on the Intended Interface

Purpose Verify that sFlow technology is enabled on 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



NOTE: The sample limit cannot be configured and is set to 300 packets/second.

Meaning The output indicates that sFlow technology is enabled on the **ge-0/0/0.0** interface with an egress sample rate of 1000, a disabled ingress sample rate, a sampling limit of 300 packets per second 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 address	Udp-port	No. of samples
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 74](#)
- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)

Configuring sFlow Technology

- [Configuring sFlow Technology for Network Monitoring \(CLI Procedure\) on page 74](#)

Configuring sFlow Technology for Network Monitoring (CLI Procedure)

You can configure sFlow technology, designed for monitoring high-speed switched or routed networks, 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* (see <http://faqs.org/rfcs/rfc3176.html>).`

To configure sFlow features:

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

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

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.

3. Specify how often the sFlow agent polls the interface:

```
[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 qualifier, or both.



NOTE: The *sample-rate number* (the global sample rate) statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.



NOTE: We recommend that you configure the same sample rates for both ingress and egress. If the sample rates are different, the lower value is used.

To specify an egress sample rate:

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

To specify an ingress sample rate:

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

5. To configure the polling interval and the egress and ingress sample 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 ip-address
```

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

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

Related Documentation

- [Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70](#)
- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)

Configuration Statements for sFlow Technology

- [\[edit protocols\] Configuration Statement Hierarchy on page 76](#)

[edit protocols] Configuration Statement Hierarchy

```
protocols {
  connections {
    remote-interface-switch connection-name {
      interface interface-name.unit-number;
      transmit-lsp label-switched-path;
      receive-lsp label-switched-path;
      no-autonegotiation;
    }
  }
  dcbx {
    disable;
    interface (all | interface-name) {
      disable;
      priority-flow-control {
        no-auto-negotiation;
      }
    }
  }
  dot1x {
    authenticator {
      authentication-profile-name profile-name;
      interface (all | [interface-names]) {
        disable;
        guest-vlan ( vlan-id | vlan-name );
        mac-radius <restrict>;
        maximum-requests number;
        no-reauthentication;
        quiet-period seconds;
        reauthentication {
```

```

        interval seconds;
    }
    retries number;
    server-fail (deny | permit | use-cache | vlan-id | vlan-name);
    server-reject-vlan (vlan-id | vlan-name) {
        eapol-block;
        block-interval block-interval;
    }
    server-timeout seconds;
    supplicant (multiple | single | single-secure);
    supplicant-timeout seconds;
    transmit-period seconds;
}
no-mac-table-binding {
    authentication-profile-name
    interface
}
static mac-address {
    interface interface-name;
    vlan-assignment (vlan-id | vlan-name);
}
igmp-snooping {
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>
        <match regex>;
        flag flag (detail | disable | receive | send);
    }
}
vlan (vlan-id | vlan-number) {
    data-forwarding {
        source {
            groups group-prefix;
        }
        receiver {
            source-vlans vlan-list;
            install ;
        }
    }
}
disable {
    interface interface-name
}
immediate-leave;
interface interface-name {
    group-limit limit;
    multicast-router-interface;
    static {
        group ip-address;
    }
}
proxy ;
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
}
}
lldp {

```

```
disable (LLDP);
advertisement-interval seconds;
hold-multiplier number;
interface (LLDP) (all | interface-name) {
    disable (LLDP);
}
lldp-configuration-notification-interval seconds;
management-address ip-management-address;
ptopo-configuration-maximum-hold-time seconds;
ptopo-configuration-trap-interval seconds;
traceoptions (LLDP) {
    file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
    flag flag (detail | disable | receive | send);
}
}
lldp-med {
    disable;
    fast-start number;
    interface (all | interface-name) {
        disable;
        location {
            elin number;
            civic-based {
                what number;
                country-code code;
                ca-type {
                    number {
                        ca-value value;
                    }
                }
            }
        }
    }
}
}
mpls {
    interface (all | interface-name);
    label-switched-path lsp-name to remote-provider-edge-switch;
    path destination {
        <address | hostname> <strict | loose>
    }
}
mstp {
    disable;
    bpdu-block-on-edge;
    bridge-priority priority;
    configuration-name name;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        arp-on-stp
        bpdu-timeout-action {
            block;
            log;
        }
        cost cost;
        disable;
```

```

    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
}
max-age seconds;
max-hops hops;
msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
        disable;
        cost cost;
        edge;
        mode mode;
        priority priority;
    }
}
revision-level revision-level;
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}
}
mvrp {
    add-attribute-length-in-pdu
    disable
    interface (all | interface-name) {
        disable;
        join-timer milliseconds;
        leave-timer milliseconds;
        leaveall-timer milliseconds;
        registration (forbidden | normal);
    }
    no-dynamic-vlan;
    traceoptions {
        file filename <files number > <size size > <no-stamp | world-readable |
        no-world-readable>;
        flag flag;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            action-profile profile-name {
                default-actions {
                    interface-down;
                }
            }
        }
        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;
        interval (10m | 10s | 1m | 1s| 100ms);
        loss-threshold number;
    }
    mep mep-id {
        auto-discovery;
        direction down;
        interface interface-name;
        remote-mep mep-id {
            action-profile profile-name;
        }
    }
}
}
}
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;
        event-thresholds threshold-value;
        remote-loopback;
        event-thresholds {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
    }
    negotiation-options {
        allow-remote-loopback;
        no-allow-link-events;
    }
}
}
}
rstp {
    disable;
    bpdu-block-on-edge;
    bridge-priority priority;
```



```

forward-delay seconds;
hello-time seconds;
interface (all | interface-name) {
    disable;
    arp-on-stp
        bpdutimeout-action {
            block;
            log;
        }
    cost cost;
    edge;
    mode mode;
    no-root-port;
    priority priority;
}
max-age seconds;
}
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
        no-world-readable>;
    flag flag;
}
}
sflow {
    agent-id;
    collector {
        ip-address;
        udp-port port-number;
    }
    disable;
    interfaces interface-name {
        disable;
        polling-interval seconds;
        sample-rate {
            egress number;
            ingress number;
        }
    }
    polling-interval seconds;
    sample-rate {
        egress number;
        ingress number;
    }
    source-ip;
}
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        arp-on-stp
            bpdutimeout-action {
                block;
                log;
            }
    }
}

```

```
    }
    cost cost;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
}
traceoptions {
  file filename <files number > <size size> <no-stamp | world-readable |
    no-world-readable>;
  flag flag;
}
uplink-failure-detection {
  group {
    group-name {
      link-to-monitor {
        interface-name;
      }
      link-to-disable {
        interface-name;
      }
    }
  }
}
vstp {
  bpdu-block-on-edge;
  disable;
  force-version stp;
  vlan (all | vlan-id | vlan-name) {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      arp-on-stp
        bpdu-timeout-action {
          log;
          block;
        }
      cost cost;
      disable;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    traceoptions {
      file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}
}
```

**Related
Documentation**

- 802.1X for EX Series Switches Overview
- Understanding Authentication on EX Series Switches
- Understanding Server Fail Fallback and Authentication on EX Series Switches
- IGMP Snooping on EX Series Switches Overview
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches
- Understanding MSTP for EX Series Switches
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches
- [Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 279](#)
- [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)
- Understanding RSTP for EX Series Switches
- Understanding STP for EX Series Switches
- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)
- Understanding VSTP for EX Series Switches
- [Understanding Uplink Failure Detection on page 329](#)
- Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches

collector

Syntax	<pre>collector { ip-address; udp-port port-number; }</pre>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 76• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74

disable

Syntax	<pre>disable;</pre>
Hierarchy Level	[edit protocols sflow], [edit protocols sflow interfaces <i>interface-name</i>]
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	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 76• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74


interfaces

Syntax	<pre> interfaces <i>interface-name</i> { disable; polling-interval <i>seconds</i>; sample-rate { egress <i>number</i>; ingress <i>number</i>; } }</pre>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	<p>Configure sFlow network traffic monitoring on the specified interface on the switch. You can configure sFlow parameters such as polling interval and sample rate with different values on different interfaces, and you can also disable sFlow monitoring on individual interfaces.</p> <p>The remaining statements are explained separately.</p>
Options	<i>interface-name</i> —Name of the interface on which to configure sFlow parameters.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • [edit protocols] Configuration Statement Hierarchy on page 76 • Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70 • Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74

polling-interval

Syntax	<code>polling-interval <i>seconds</i>;</code>
Hierarchy Level	[edit protocols sflow], [edit protocols sflow interfaces <i>interface-name</i>]
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’s 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 for the global sFlow configuration. If no global interval is configured, the switch waits 20 seconds between messages.
Options	<i>seconds</i> —Number of seconds between port statistics update messages. A 0 (zero) value specifies that polling is disabled. Range: 0–3600 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	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 76• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70

sample-rate

Syntax	sample-rate { egress <i>number</i> ; ingress <i>number</i> ; }
Hierarchy Level	[edit protocols sflow], [edit protocols sflow interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches. Option <i>number</i> (directly following sample-rate) deprecated and options egress <i>number</i> and ingress <i>number</i> added in Junos OS Release 10.4 for EX Series switches.
Description	Set the ratios of the number of packets to be sampled in sFlow network traffic monitoring. For example, if you specify a rate of 1000, every thousandth packet (1 packet out of 1000) is sampled.
Default	By default, both ingress and egress sample rates are disabled if no global sample rate is configured.
<div>  <p>NOTE: The sample-rate <i>number</i> (the global sample-rate) statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.</p> </div>	
Options	egress <i>number</i> —Egress qualifier for the sample rate. Range: 100–1073741823 Default: 2048 ingress <i>number</i> —Ingress qualifier for the sample rate. Range: 100–1073741823 Default: 2048
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • [edit protocols] Configuration Statement Hierarchy on page 76 • Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74 • Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70

sflow

Syntax	<pre>sflow { agent-id <i>ip-address</i>; collector { <i>ip-address</i>; udp-port <i>port-number</i>; } disable; interfaces <i>interface-name</i> { disable; polling-interval <i>seconds</i>; sample-rate <i>number</i>; } polling-interval <i>seconds</i>; sample-rate <i>number</i>; source-ip <i>ip-address</i>; }</pre>
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	<p>Configure sFlow technology, designed for monitoring high-speed switched or routed networks, to continuously monitor traffic at wire speed on specified interfaces simultaneously. sFlow data can be used to provide network traffic visibility information.</p> <p>The remaining statements are explained separately.</p>
Default	The sFlow protocol 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	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 76• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74

udp-port

Syntax	<code>udp-port <i>port-number</i>;</code>
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	<i>port-number</i> —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	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 76• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74

Operational Commands for sFlow Technology

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	<p>none—Display default sFlow technology configuration information.</p> <p>collector—(Optional) Display standard status information about the specified sFlow collector.</p> <p>interface—(Optional) Display standard status information about the specified sFlow interface.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show sflow interface on page 93 • show sflow collector on page 92 • Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70 • Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74
List of Sample Output	show sflow on page 91
Output Fields	Table 5 on page 90 lists the output fields for the show sflow command. Output fields are listed in the approximate order in which they appear.

Table 5: 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 sample limit cannot be configured and is set to 300 packets/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

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
```

show sflow collector

Syntax	show sflow collector
Release Information	Command introduced in Junos OS Release 9.3 for EX Series switches.
Description	Displays a list of configured sFlow collectors and their properties.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show sflow on page 90 • show sflow interface on page 93 • Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70 • Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74
List of Sample Output	show sflow collector on page 92
Output Fields	Table 6 on page 92 lists the output fields for the show sflow collector command. Output fields are listed in the approximate order in which they appear.

Table 6: 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	Packet sampling rate.	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
```

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	<ul style="list-style-type: none"> • show sflow on page 90 • show sflow collector on page 92 • Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 70 • Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 74
List of Sample Output	show sflow interface on page 93
Output Fields	Table 7 on page 93 lists the output fields for the show sflow interface command. Output fields are listed in the approximate order in which they appear.

Table 7: 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 sample rate is enabled.	All levels
Status Ingress	Indicates whether ingress sample rate is enabled.	All levels
Sample rate Egress	Rate at which egress packets are sampled.	All levels
Sample rate Ingress	Rate at which ingress packets are sampled.	All levels
Adapted sample rate Egress	Adapted rate at which egress packets are sampled.	All levels
Adapted sample rate Ingress	Adapted rate at which ingress packets are sampled.	All levels
Polling-interval	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
              Egress Ingress  Egress Ingress  Egress Ingress
ge-0/0/0.0    Enabled Disabled  1000   2048    1000   2048
                                         20
```


CHAPTER 3

SNMP

- [Configuring SNMP on page 95](#)
- [Configuration Statements for SNMP on page 98](#)
- [Operational Commands for SNMP on page 163](#)

Configuring SNMP

- [Configuring SNMP \(J-Web Procedure\) on page 95](#)

Configuring SNMP (J-Web Procedure)

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 8 on page 95](#).
3. To apply the configuration click **Apply**.



NOTE: After you make changes to the configuration in 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 8: 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).

Table 8: 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. 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		
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		
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.

Table 8: SNMP Configuration Page (*continued*)

Field	Function	Your Action
Categories	Specifies which trap categories are added to the trap group being configured.	<ul style="list-style-type: none"> To generate traps for authentication failures, select Authentication. To generate traps for chassis and environment notifications, select Chassis. To generate traps for configuration changes, select Configuration. To generate traps for link-related notifications (up-down transitions), select Link. To generate traps for remote operation notifications, select Remote operations. To generate traps for remote network monitoring (RMON), select RMON alarm. To generate traps for routing protocol notifications, select Routing. To generate traps on system warm and cold starts, select Startup. 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.	<ol style="list-style-type: none"> Enter the hostname or IP address, in dotted decimal notation, of the target system to receive the SNMP traps. Click Add.
Health Monitoring		
Enable Health Monitoring	<p>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:</p> <ul style="list-style-type: none"> Percentage of file storage used Percentage of Routing Engine CPU used Percentage of Routing Engine memory used Percentage of memory used for each system process Percentage of CPU used by the forwarding process Percentage of memory used for temporary storage by the forwarding process 	<p>Select the check box to enable the health monitor and configure options. Clear the check box to disable the health monitor.</p> <p>NOTE: If you select the Enable Health Monitoring check box and do not specify options, then SNMP health monitoring is enabled with default values.</p>
Interval	<p>Specifies the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds.</p> <p>For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.</p>	<p>Enter an interval time, in seconds, from 1 through 2147483647.</p> <p>The default value is 300 seconds (5 minutes).</p>

Table 8: SNMP Configuration Page (*continued*)

Field	Function	Your Action
Rising Threshold	<p>Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is increasing.</p> <p>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.</p>	<p>Enter a value from 0 through 100. The default value is 90.</p>
Falling Threshold	<p>Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is decreasing.</p> <p>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.</p>	<p>Enter a value from 0 through 100. The default value is 80.</p> <p>NOTE: The falling threshold value must be less than the rising threshold value.</p>

- Related Documentation**
- [Monitoring System Process Information](#)
 - [Monitoring System Properties](#)

Configuration Statements for SNMP

- [\[edit snmp\] Configuration Statement Hierarchy on page 98](#)

[edit snmp] Configuration Statement Hierarchy

```
snmp {
  rmon {
    history index {
      bucket-size number;
      interface interface-name;
      interval seconds;
      owner owner-name;
    }
  }
}
```

- Related Documentation**
- [Configuring SNMP \(J-Web Procedure\) on page 95](#)
 - [Junos OS Network Management Configuration Guide](#)

address

Syntax	<code>address <i>address</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
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	<i>address</i> —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	<ul style="list-style-type: none"> Configuring the Address

address-mask

Syntax	<code>address-mask <i>address-mask</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Verify the source addresses for a group of target addresses.
Options	<i>address-mask</i> 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	<ul style="list-style-type: none"> Configuring the Address Mask

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	<ul style="list-style-type: none">Configuring the Agent Address for SNMP Traps

alarm

Syntax	<pre>alarm <i>index</i> { <i>description</i> <i>description</i>; <i>falling-event-index</i> <i>index</i>; <i>falling-threshold</i> <i>integer</i>; <i>falling-threshold-interval</i> <i>seconds</i>; <i>interval</i> <i>seconds</i>; <i>request-type</i> (get-next-request get-request walk-request); <i>rising-event-index</i> <i>index</i>; <i>rising-threshold</i> <i>integer</i>; <i>sample-type</i> (absolute-value delta-value); <i>startup-alarm</i> (falling-alarm rising-alarm rising-or-falling alarm); <i>syslog-subtag</i> <i>syslog-subtag</i>; <i>variable</i> <i>oid-variable</i>; }</pre>
Hierarchy Level	[edit snmp rmon]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure RMON alarm entries.
Options	<p><i>index</i>—Identifies this alarm entry as an integer.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring an Alarm Entry and Its Attributes event on page 112

authorization

Syntax	<code>authorization <i>authorization</i>;</code>
Hierarchy Level	[edit <code>snmp community <i>community-name</i></code>]
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	<i>authorization</i> —Access authorization level: <ul style="list-style-type: none">• 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: <code>read-only</code>
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the SNMP Community String

bucket-size

Syntax	<code>bucket-size <i>number</i>;</code>
Hierarchy Level	[edit <code>snmp rmon history</code>]
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	<i>number</i> —Number of discrete samples of Ethernet statistics requested.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SNMP (J-Web Procedure) on page 95• Junos OS Network Management Configuration Guide

categories

Syntax	<code>categories { category; }</code>
Hierarchy Level	<code>[edit snmp trap-group group-name]</code>
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 , 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	<ul style="list-style-type: none"> Configuring SNMP Trap Groups

client-list

Syntax	<code>client-list client-list-name { ip-addresses; }</code>
Hierarchy Level	<code>[edit snmp]</code>
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX 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	<ul style="list-style-type: none"> Adding a Group of Clients to an SNMP Community

client-list-name

Syntax	<code>client-list-name <i>client-list-name</i>;</code>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>]</code>
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	<i>client-list-name</i> —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	<ul style="list-style-type: none">Adding a Group of Clients to an SNMP Community

clients

Syntax	<pre>clients { <i>address</i> <restrict>; }</pre>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>]</code>
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	<i>address</i> —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 <i>address</i> options. <i>restrict</i> —(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	<ul style="list-style-type: none">Configuring the SNMP Community String

commit-delay

Syntax	commit-delay <i>seconds</i> ;
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	<i>seconds</i> —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	<ul style="list-style-type: none">Configuring the Commit Delay Timer


community

Syntax	<pre>community <i>community-name</i> { authorization <i>authorization</i>; client-list-name <i>client-list-name</i>; clients { address restrict; } view <i>view-name</i>; }</pre>
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	<p>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.</p> <p>The SNMP client application specifies an SNMP community name in Get, GetBulk, GetNext, and Set SNMP requests.</p>
Default	If you omit the community statement, all SNMP requests are denied.
Options	<p><i>community-name</i>—Community string. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">Configuring the SNMP Community String

community

Syntax	<code>community <i>community-name</i>;</code>
Hierarchy Level	[edit snmp rmon event <i>index</i>]
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	<i>community-name</i> —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	<ul style="list-style-type: none">Configuring an Event Entry and Its Attributes

community-name

Syntax	<code>community-name <i>community-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 snmp-community <i>community-index</i>]</code>
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	<i>community-name</i> —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 (" ").
<div> NOTE: Community names must be unique. You cannot configure the same community name at the <code>[edit snmp community]</code> and <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy levels.</div> <div>The community name at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level is encrypted and not displayed in the command-line interface (CLI).</div>	
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the SNMPv3 Community

contact

Syntax	<code>contact <i>contact</i>;</code>
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	<ul style="list-style-type: none"> Configuring the System Contact on a Device Running Junos OS

description

Syntax	<code>description <i>description</i>;</code>
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	<ul style="list-style-type: none"> Configuring the System Description on a Device Running Junos OS


description

Syntax	<code>description <i>description</i>;</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>], [edit snmp rmon event <i>index</i>]
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	<i>description</i> —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	<ul style="list-style-type: none">Configuring the DescriptionConfiguring an Event Entry and Its Attributes

destination-port

Syntax	<code>destination-port <i>port-number</i>;</code>
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	<i>port-number</i> —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	<ul style="list-style-type: none">Configuring SNMP Trap Groups

engine-id

Syntax	engine-id { (local <i>engine-id-suffix</i> 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, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> . You can configure the suffix here.
<div>  <p>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.</p> <p>For the engine ID, we recommend using the MAC address of fxp0.</p> </div>	
Options	<p>local <i>engine-id-suffix</i>—Explicit setting for the engine ID suffix.</p> <p>use-default-ip-address—The engine ID suffix is generated from the default IP address.</p> <p>use-mac-address—The SNMP engine identifier is generated from the MAC address of the management interface on the router.</p> <p>Default: use-default-ip-address</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the Local Engine ID

event

Syntax	<pre>event <i>index</i> { community <i>community-name</i>; description <i>description</i>; type <i>type</i>; }</pre>
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	<ul style="list-style-type: none">Configuring an Event Entry and Its Attributesalarm on page 101

falling-event-index

Syntax	<pre>falling-event-index <i>index</i>;</pre>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
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	<ul style="list-style-type: none">Configuring the Falling Event Index or Rising Event Indexrising-event-index on page 133

falling-threshold

Syntax	<code>falling-threshold <i>percentage</i>;</code>
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	<i>percentage</i> —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	<ul style="list-style-type: none">Configuring the Falling Threshold or Rising Thresholdrising-threshold on page 134

falling-threshold

Syntax	<code>falling-threshold <i>integer</i>;</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
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	<i>integer</i> —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	<ul style="list-style-type: none">Configuring the Falling Threshold or Rising Thresholdrising-threshold on page 135

falling-threshold-interval

Syntax	<code>falling-threshold-interval <i>seconds</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm index]</code>
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	<i>seconds</i> —Time between samples, in seconds. Range: 1 through 2,147,483,647 seconds Default: 60 seconds
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Falling Threshold Interval interval on page 122

filter-duplicates

Syntax	<code>filter-duplicates;</code>
Hierarchy Level	<code>[edit snmp]</code>
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	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Filtering Duplicate SNMP Requests

filter-interfaces

Syntax	<pre>filter-interfaces { interfaces { all-internal-interfaces; interface 1; interface 2; } }</pre>
Hierarchy Level	[edit snmp]
Release Information	<p>Statement introduced in Junos OS Release 9.4.</p> <p>Statement introduced in Junos OS Release 9.4 for EX Series Switches.</p>
Description	Filter out information related to specific interfaces from the output of SNMP Get and GetNext requests performed on interface-related MIBs.
Options	<p>all-internal-interfaces—Filters out information from SNMP Get and GetNext requests for the specified interfaces.</p> <p>interfaces—Specifies the interfaces to filter out from the output of SNMP Get and GetNext requests.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Filtering Interface Information Out of SNMP Get and GetNext Output

group (Configuring Group Name)

```
Syntax  group group-name {
        (default-context-prefix | context-prefix context-prefix){
            security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                }
            }
        }
    }
```

Hierarchy Level [edit snmp v3 vacm access]

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

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. 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.

The remaining statements under this hierarchy are documented in separate topics.

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

group (Defining Access Privileges for an SNMPv3 Group)

Syntax	<code>group <i>group-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 vacm security-to-group security-model (usm v1 v2c) <i>security-name security-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Define access privileges granted to a group.
Options	<i>group-name</i> —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	<ul style="list-style-type: none">Configuring the Group

health-monitor

Syntax	<code>health-monitor { <i>falling-threshold percentage</i>; <i>interval seconds</i>; <i>rising-threshold percentage</i>; }</code>
Hierarchy Level	<code>[edit snmp]</code>
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	<ul style="list-style-type: none">Configuring Health Monitoring on Devices Running Junos OS

history

Syntax	<pre>history <i>history-index</i> { <i>bucket-size</i> <i>number</i>; interface <i>interface-name</i>; interval <i>seconds</i>; owner <i>owner-name</i>; }</pre>
Hierarchy Level	[edit snmp rmon]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>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.</p> <p>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 <i>interface-name</i> statement is mandatory. Other statements in the history group are optional.</p>
Default	Not configured.
Options	<p><i>history-index</i>—Identifies this history entry as an integer.</p> <p>Range: 1 through 65535</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring SNMP (J-Web Procedure) on page 95 Junos OS Network Management Configuration Guide

interface

Syntax	<code>interface [<i>interface-names</i>];</code>
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	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	<i>interface-names</i> —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	<ul style="list-style-type: none">Configuring the Interfaces on Which SNMP Requests Can Be Accepted

interface

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	[edit snmp rmon history <i>history-index</i>]
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	<i>interface-name</i> —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	<ul style="list-style-type: none">Configuring SNMP (J-Web Procedure) on page 95Junos OS Network Management Configuration Guide

interval

Syntax	<code>interval seconds;</code>
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	<i>seconds</i> —Interval at which data is to be sampled for the specified interface.
Required Privilege	snmp—To view this statement in the configuration.
Level	snmp-control—To add this statement to the configuration.

interval

Syntax	<code>interval seconds;</code>
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	<i>seconds</i> —Time between samples, in seconds. Range: 1 through 2147483647 seconds Default: 300 seconds
Required Privilege	snmp—To view this statement in the configuration.
Level	snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Interval


interval

Syntax	<code>interval seconds;</code>
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	<ul style="list-style-type: none">Configuring the Interval

location

Syntax	<code>location location;</code>
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	<ul style="list-style-type: none">Configuring the System Location for a Device Running Junos OS

logical-system

Syntax	<pre>logical-system <i>logical-system-name</i> { <i>routing-instance routing-instance-name</i>; }</pre>
Hierarchy Level	<pre>[edit snmp <i>community community-name</i>], [edit snmp <i>trap-group</i>], [edit snmp <i>trap-options</i>] [edit snmp <i>v3target-address target-address-name</i>]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.3</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
	<div>  <p>NOTE: The <code>logical-system</code> statement replaces the <code>logical-router</code> statement, and is backward-compatible with Junos OS Release 8.3 and later.</p> </div>
Description	<p>Specify a logical system name for SNMP v1 and v2c clients.</p> <p>Include at the <code>[edit snmp trap-options]</code> hierarchy level to specify a logical-system address as the source address of an SNMP trap.</p> <p>Include at the <code>[edit snmp v3 target-address]</code> hierarchy level to specify a logical-system name as the destination address for an SNMPv3 trap or inform.</p>
Options	<p><i>logical-system-name</i>—Name of the logical system.</p> <p><i>routing-instance routing-instance-name</i>—Statement to specify a routing instance associated with the logical system.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community Configuring the Trap Target Address

message-processing-model

Syntax	<code>message-processing-model (v1 v2c v3);</code>
Hierarchy Level	<code>[edit snmp v3 target-parameters <i>target-parameter-name</i> parameters]</code>
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	<code>v1</code> —SNMPv1 message process model. <code>v2c</code> —SNMPv2c message process model. <code>v3</code> —SNMPv3 message process model.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Message Processing Model

name

Syntax	<code>name <i>name</i>;</code>
Hierarchy Level	<code>[edit snmp]</code>
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	<code>name</code> —System name override.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the System Name

nonvolatile

Syntax	<code>nonvolatile { commit-delay <i>seconds</i>; }</code>
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	<ul style="list-style-type: none">Configuring the Commit Delay Timercommit-delay on page 105

notify

Syntax	<pre>notify <i>name</i> { tag <i>tag-name</i>; type (trap inform); }</pre>
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.
Description	Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.
Options	<p><i>name</i>—Name assigned to the notification.</p> <p><i>tag-name</i>—Notifications are sent to all targets configured with this tag.</p> <p><i>type</i>—Notification type is trap or inform. Traps are unconfirmed notifications. Informs are confirmed notifications.</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Inform Notification Type and Target AddressConfiguring the SNMPv3 Trap Notification

notify-filter (Configuring the Profile Name)

Syntax	<code>notify-filter <i>profile-name</i> { oid <i>oid</i> (include exclude); }</code>
Hierarchy Level	[edit snmp v3]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	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	<i>profile-name</i> —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	<ul style="list-style-type: none"> Configuring the Trap Notification Filter oid on page 129

notify-filter (Applying to the Management Target)

Syntax	<code>notify-filter <i>profile-name</i>;</code>
Hierarchy Level	[edit snmp v3 target-parameters <i>target-parameters-name</i>]
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 notify filter to be used by a specific set of target parameters.
Options	<i>profile-name</i> —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	<ul style="list-style-type: none"> Applying the Trap Notification Filter

notify-view

Syntax	<code>notify-view <i>view-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</i>) security-model (any usm v1 v2c) security-level (authentication none privacy)]</code>
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 notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).
Options	<i>view-name</i> —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	<ul style="list-style-type: none">Configuring MIB ViewsConfiguring the Notify View

oid

Syntax	<code>oid <i>object-identifier</i> (exclude include);</code>
Hierarchy Level	<code>[edit snmp view <i>view-name</i>]</code>
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. <i>object-identifier</i> —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	<ul style="list-style-type: none">Configuring MIB Views

oid

Syntax	<code>oid <i>oid</i> (include exclude);</code>
Hierarchy Level	<code>[edit snmp v3 notify-filter <i>profile-name</i>]</code>
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	<p>exclude—Exclude the subtree of MIB objects represented by the specified OID.</p> <p>include—Include the subtree of MIB objects represented by the specified OID.</p> <p>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.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the Trap Notification Filter

owner

Syntax	<code>owner <i>owner-name</i>;</code>
Hierarchy Level	<code>[edit snmp rmon history]</code>
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	<p>owner-name—The user or group responsible for this configuration.</p> <p>Range: 0 through 32 alphanumeric characters</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring SNMP (J-Web Procedure) on page 95 Junos OS Network Management Configuration Guide

parameters

Syntax	<pre>parameters { message-processing-model (v1 v2c v3); security-level (none authentication privacy); security-model (usm v1 v2c); security-name security-name; }</pre>
Hierarchy Level	[edit snmp v3 target-parameters <i>target-parameters-name</i>]
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	<ul style="list-style-type: none">Defining and Configuring the Trap Target Parameters

port

Syntax	<pre>port port-number;</pre>
Hierarchy Level	[edit snmp v3 target-address <i>target-address-name</i>]
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	<i>port-number</i> —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	<ul style="list-style-type: none">Configuring the Port

read-view

Syntax	<code>read-view <i>view-name</i>;</code>
Hierarchy Level	[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</i>) 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	<i>view-name</i> —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	<ul style="list-style-type: none">Configuring the Read ViewConfiguring MIB Views

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	<ul style="list-style-type: none">Configuring the Request Typevariable on page 161

rising-event-index

Syntax	<code>rising-event-index <i>index</i>;</code>
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	<i>index</i> —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	<ul style="list-style-type: none">Configuring the Falling Event Index or Rising Event Indexfalling-event-index on page 112

rising-threshold

Syntax	<code>rising-threshold <i>percentage</i>;</code>
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	<i>percentage</i> —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	<ul style="list-style-type: none">• falling-threshold on page 113• Configuring the Falling Threshold or Rising Threshold

rising-threshold

Syntax	<code>rising-threshold <i>integer</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
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	<i>integer</i> —The lower threshold for the alarm entry. Range: –2,147,483,648 through 2,147,483,647
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Falling Threshold or Rising Threshold falling-threshold on page 114

rmon

Syntax	<code>rmon { ... }</code>
Hierarchy Level	<code>[edit snmp]</code>
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	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring an Alarm Entry and Its Attributes

rmon

Syntax	<pre>rmon { history <i>history-index</i> { interface <i>interface-name</i>; bucket-size <i>number</i>; interval <i>seconds</i>; owner <i>owner-name</i>; } }</pre>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>RMON is an existing feature of Junos OS.</p> <p>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.</p> <p>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.</p> <p>The statements are explained separately.</p>
Default	Disabled.
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring SNMP (J-Web Procedure) on page 95• Junos OS Network Management Configuration Guide

routing-instance

Syntax	<code>routing-instance <i>routing-instance-name</i>;</code>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>],</code> <code>[edit snmp community <i>community-name</i> logical-system <i>logical-system-name</i>],</code> <code>[edit snmp trap-group <i>group</i>]</code>
Release Information	Statement introduced in Junos OS Release 8.3. Added to the <code>[edit snmp community <i>community-name</i>]</code> hierarchy level in Junos OS Release 8.4. Added to the <code>[edit snmp community <i>community-name</i> logical-system <i>logical-system-name</i>]</code> 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 <i>logical-system-name</i> statement at the <code>[edit snmp community <i>community-name</i>]</code> hierarchy level and specify the routing-instance statement under the <code>[edit snmp community <i>community-name</i> logical-system <i>logical system-name</i>]</code> hierarchy level.
Options	<i>routing-instance-name</i> —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	<ul style="list-style-type: none"> Configuring SNMP Trap Groups Configuring the Source Address for SNMP Traps Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community

routing-instance

Syntax	<code>routing-instance <i>routing-instance-name</i>;</code>
Hierarchy Level	[edit snmp v3 target-address <i>target-address-name</i>]
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	<p><i>routing-instance-name</i>—Name of the routing instance.</p> <p>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).</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Trap Target Address

sample-type

Syntax	<code>sample-type (absolute-value delta-value);</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
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	<p>absolute-value—Actual value of the selected variable is used when comparing against the thresholds.</p> <p>delta-value—Difference between samples of the selected variable is used when comparing against the thresholds.</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Sample Type

security-level (Generating SNMP Notifications)

Syntax	security-level (authentication none privacy);
Hierarchy Level	[edit snmp v3 target-parameters <i>target-parameters-name</i> 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	<ul style="list-style-type: none">Configuring the Security Level

security-level (Defining Access Privileges)

Syntax	<code>security-level (authentication none privacy) { notify-view <i>view-name</i>; read-view <i>view-name</i>; write-view <i>view-name</i>; }</code>
Hierarchy Level	<code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</i>) security-model (any usm v1 v2c)]</code>
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	<code>none</code>
Options	<code>authentication</code> —Provide authentication but no encryption. <code>none</code> —No authentication and no encryption. <code>privacy</code> —Provide authentication and encryption.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Security Level

security-model (Access Privileges)

Syntax	security-model (usm v1 v2c);
Hierarchy Level	[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</i>)]
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	<ul style="list-style-type: none">Configuring the Security Model

security-model (Group)

Syntax	<pre>security-model (usm v1 v2c) { security-name security-name { group group-name; } }</pre>
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	<ul style="list-style-type: none">Configuring the Security Model

security-model (SNMP Notifications)

Syntax	<pre>security-model (usm v1 v2c);</pre>
Hierarchy Level	[edit snmp v3 target-parameters <i>target-parameters-name</i> 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	<ul style="list-style-type: none">Configuring the Security Model

security-name (Security Group)

Syntax	<code>security-name <i>security-name</i> { <i>group</i> <i>group-name</i>; }</code>
Hierarchy Level	[edit snmp v3 vacm security-to-group <i>security-model</i> (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	<i>security-name</i> —Username configured at the [edit snmp v3 usm local-engine user <i>username</i>] hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the [edit snmp v3 snmp-community <i>community-index</i>] hierarchy level.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Assigning Security Names to Groups

security-name (Community String)


Syntax	<code>security-name <i>security-name</i>;</code>
Hierarchy Level	[edit snmp v3 <i>snmp-community</i> <i>community-index</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Associate the community string configured at the [edit snmp v3 snmp-community <i>community-index</i>] hierarchy level to a security name.
Options	<i>security-name</i> —Name used when performing 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	<ul style="list-style-type: none"> Configuring the Security Names

security-name (SNMP Notifications)

Syntax	<code>security-name <i>security-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]</code>
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	<i>security-name</i> —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.
<div> NOTE: The access privileges for the group associated with this security name must allow this notification to be sent.</div> <p>If you are using the v1 or v2 security models, the security name at the <code>[edit snmp v3 vacm security-to-group]</code> hierarchy level must match the security name at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level.</p>	
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Security Name

security-to-group

Syntax	<pre>security-to-group { security-model (usm v1 v2c) { group group-name; security-name security-name; } }</pre>
Hierarchy Level	[edit snmp v3 vacm]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	<p>Configure the group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Assigning Security Model and Security Name to a Group

snmp

Syntax	snmp { ... }
Hierarchy Level	[edit]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure SNMP.
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring SNMP on a Device Running Junos OS

snmp

Syntax	<pre>snmp { rmon { history index { interface interface-name; bucket-size number; interval seconds; owner owner-name; } } }</pre>
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	<ul style="list-style-type: none">• Configuring SNMP (J-Web Procedure) on page 95

snmp-community

Syntax	<pre>snmp-community community-index { community-name community-name; security-name security-name; tag tag-name; }</pre>
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	<ul style="list-style-type: none">• Configuring the SNMPv3 Community

source-address

Syntax	source-address <i>address</i> ;
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	<ul style="list-style-type: none">Configuring the Source Address for SNMP Traps

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	<p>falling-alarm—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.</p> <p>rising-alarm—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.</p> <p>rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.</p> <p>Default: rising-or-falling-alarm</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Sample Type

syslog-subtag

Syntax	syslog-subtag <i>syslog-subtag</i> ;
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	<p>syslog-subtag <i>syslog-subtag</i>—Tag of not more than 80 uppercase characters to be added to syslog messages.</p> <p>Default: None</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the System Log Tag

tag

Syntax	<code>tag tag-name;</code>
Hierarchy Level	[edit snmp v3 notify <i>name</i>], [edit snmp v3 snmp-community <i>community-index</i>]
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	<ul style="list-style-type: none"> Configuring the Tag Configuring the SNMPv3 Trap Notification

tag-list

Syntax	<code>tag-list tag-list;</code>
Hierarchy Level	[edit snmp v3 target-address <i>target-address-name</i>]
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	<ul style="list-style-type: none"> Configuring the Trap Target Address

target-address

Syntax	<pre>target-address <i>target-address-name</i> { address <i>address</i>; address-mask <i>address-mask</i>; logical-system <i>logical-system</i>; port <i>port-number</i>; retry-count <i>number</i>; routing-instance <i>instance</i>; tag-list <i>tag-list</i>; target-parameters <i>target-parameters-name</i>; timeout <i>seconds</i>; }</pre>
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	<p><i>target-address-name</i>—String that identifies the target address.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Trap Target Address

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

targets

Syntax	<code>targets { <code>address</code>; }</code>
Hierarchy Level	<code>[edit snmp trap-group <i>group-name</i>]</code>
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	<i>address</i> —IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring SNMP Trap Groups

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } </pre>
Hierarchy Level	[edit snmp]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>file <i>filename</i> option added in Junos OS Release 8.1.</p> <p>world-readable no-world-readable option added in Junos OS Release 8.1.</p> <p>match <i>regular-expression</i> option added in Junos OS Release 8.1.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>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:</p> <ul style="list-style-type: none"> • chassisd • craftd • ilmids • mib2d • rmopd • serviced • snmpd
Options	<p>file <i>filename</i>—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.</p> <p>files <i>number</i>—(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.</p> <p>Range: 2 through 1000 files</p> <p>Default: 10 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:</p> <ul style="list-style-type: none"> • all—Log all SNMP events. • configuration—Log reading of configuration at the [edit snmp] hierarchy level.

- **database**—Log events involving storage and retrieval in the events database.
- **events**—Log important events.
- **general**—Log general events.
- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **policy**—Log policy processing.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **server**—Log communication with processes that are generating events.
- **subagent**—Log subagent restarts.
- **timer-events**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

Range: 10 KB through 1 GB

Default: 1000 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

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

Related Documentation	• Tracing SNMP Activity on a Device Running Junos OS
------------------------------	--

trap-group

Syntax	<pre> trap-group <i>group-name</i> { categories { <i>category</i>; } destination-port <i>port-number</i>; routing-instance <i>instance</i>; targets { <i>address</i>; } version (all v1 v2); } </pre>
Hierarchy Level	[edit snmp]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
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	<p><i>group-name</i>—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring SNMP Trap Groups

trap-options

Syntax	<pre>trap-options { agent-address outgoing-interface; source-address address; }</pre>
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	<p>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.</p> <p>The remaining statements are explained separately.</p>
Default	Disabled
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring SNMP Trap Options

type

Syntax	<pre>type (inform trap);</pre>
Hierarchy Level	[edit snmp v3 notify <i>name</i>]
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	<p>inform—Defines the type of notification as an inform. SNMP informs are confirmed notifications.</p> <p>trap—Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring SNMP InformsConfiguring the SNMPv3 Trap Notification

type

Syntax	<code>type type;</code>
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	<p>type—Type of notification:</p> <ul style="list-style-type: none">• 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. <p>Default: log-and-trap</p>
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an Event Entry and Its Attributes

v3

```

Syntax  v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance instance;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);
            security-model (usm | v1 | v2c);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-sha {
                    authentication-password authentication-password;
                }
                authentication-none;
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
            }
        }
    }
}

```

```

        privacy-none;
    }
}
remote-engine engine-id {
    user username {
        authentication-md5 {
            authentication-password authentication-password;
        }
        authentication-sha {
            authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
            privacy-password privacy-password;
        }
        privacy-des {
            privacy-password privacy-password;
        }
        privacy-3des {
            privacy-password privacy-password;
        }
        privacy-none {
            privacy-password privacy-password;
        }
    }
}
}
}
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix) {
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
}
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
}
}
}

```

Hierarchy Level [edit snmp]

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

Description	Configure SNMPv3. The remaining statements are explained separately.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Minimum SNMPv3 Configuration on a Device Running Junos OS

vacm

Syntax	<pre>vacm { access { group group-name { (default-context-prefix context-prefix <i>context-prefix</i>){ 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; } } }</pre>
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	<ul style="list-style-type: none">Defining Access Privileges for an SNMP Group

variable

Syntax	<code>variable <i>oid-variable</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
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	<i>oid-variable</i> —OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, 1.3.6.1.2.1.2.2.1.10.1). Alternatively, use the MIB object name (for example, <code>ifInOctets.1</code>).
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Variable

version

Syntax	<code>version (all v1 v2);</code>
Hierarchy Level	<code>[edit snmp trap-group <i>group-name</i>]</code>
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	<code>all</code> —Send an SNMPv1 and SNMPv2 trap for every trap condition.
Options	<code>all</code> —Send an SNMPv1 and SNMPv2 trap for every trap condition. <code>v1</code> —Send SNMPv1 traps only. <code>v2</code> —Send SNMPv2 traps only.
Required Privilege Level	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring SNMP Trap Groups

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 106](#)

view (Associating a MIB View with a Community)

Syntax	<code>view <i>view-name</i>;</code>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>]</code>
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	<i>view-name</i> —Name of the view. You must use a view name already configured in the view statement at the <code>[edit snmp]</code> hierarchy level.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the SNMP Community String

write-view

Syntax	<code>write-view <i>view-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</i>) security-model (any usm v1 v2c) security-level (authentication none privacy)]</code>
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.
Description	Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).
Options	<i>view-name</i> —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	<ul style="list-style-type: none"> Configuring MIB Views Configuring the Write View

Operational Commands for SNMP

clear snmp rmon history

Syntax	clear snmp rmon history < <i>interface-name</i> all>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Delete the samples of Ethernet statistics collected, but do not delete the RMON history configuration.</p> <p>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.</p>
Options	<p><i>interface-name</i>—Delete the samples of Ethernet statistics collected for this interface.</p> <p>all—Delete the samples of Ethernet statistics collected for all interfaces that have been configured for RMON monitoring.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show snmp rmon history on page 186

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.
Description	Clear Simple Network Management Protocol (SNMP) statistics.
Options	This command has no options.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show snmp statistics on page 190
List of Sample Output	clear snmp statistics on page 165
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
```

Sample Output

```
request snmp user@host> request snmp spoof-trap xx
spoof-trap (Illegal Trap Name) Spoof trap request result: trap not found
```

Allowed Traps:

- adslAtucInitFailureTrap
- adslAtucPerfFESThreshTrap
- adslAtucPerfLofsThreshTrap
- adslAtucPerfLossThreshTrap
- adslAtucPerfLprsThreshTrap
- adslAtucRateChangeTrap
- adslAturPerfFESThreshTrap
- adslAturPerfLofsThreshTrap
- adslAturPerfLossThreshTrap
- adslAturPerfLprsThreshTrap

```

ads1AturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
d1swTrapCircuitDown
d1swTrapCircuitUp
d1swTrapTConnDown
d1swTrapTConnPartnerReject
d1swTrapTConnProtViolation
d1swTrapTConnUp
dsx1LineStatusChange
dsx3LineStatusChange
entConfigChange
fallingAlarm
frDLCIStatusChange
ggsnTrapChanged
ggsnTrapCleared
ggsnTrapNew
gmp1sTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisIDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAccessAuthServerDisabled
jnxAccessAuthServerEnabled
jnxAccessAuthServiceDown
jnxAccessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared
jnxCollFtpSwitchover
jnxCollMemoryAvailable
jnxCollMemoryUnavailable
jnxCollUnavailableDest

```


jnxCollUnavailableDestCleared
jnxCollUnsuccessfulTransfer
jnxDfcHardMemThresholdExceeded
jnxDfcHardMemUnderThreshold
jnxDfcHardPpsThresholdExceeded
jnxDfcHardPpsUnderThreshold
jnxDfcSoftMemThresholdExceeded
jnxDfcSoftMemUnderThreshold
jnxDfcSoftPpsThresholdExceeded
jnxDfcSoftPpsUnderThreshold
jnxEventTrap
jnxExampleStartup
jnxFEBSwitchover
jnxFanFailure
jnxFanOK
jnxFruCheck
jnxFruFailed
jnxFruInsertion
jnxFruOK
jnxFruOffline
jnxFruOnline
jnxFruPowerOff
jnxFruPowerOn
jnxFruRemoval
jnxHardDiskFailed
jnxHardDiskMissing
jnxJsAvPatternUpdateTrap
jnxJsChassisClusterSwitchover
jnxJsFwAuthCapacityExceeded
jnxJsFwAuthFailure
jnxJsFwAuthServiceDown
jnxJsFwAuthServiceUp
jnxJsNatAddrPoolThresholdStatus
jnxJsScreenAttack
jnxJsScreenCfgChange
jnxLdpLspDown
jnxLdpLspUp
jnxLdpSesDown
jnxLdpSesUp
jnxMIMstCistPortLoopProtectStateChangeTrap
jnxMIMstCistPortRootProtectStateChangeTrap
jnxMIMstErrTrap
jnxMIMstGenTrap
jnxMIMstInvalidBpduRxdTrap
jnxMIMstMstiPortLoopProtectStateChangeTrap
jnxMIMstMstiPortRootProtectStateChangeTrap
jnxMIMstNewRootTrap
jnxMIMstProtocolMigrationTrap
jnxMIMstRegionConfigChangeTrap
jnxMIMstTopologyChgTrap
jnxMacChangedNotification
jnxMplsLdpInitSesThresholdExceeded
jnxMplsLdpPathVectorLimitMismatch
jnxMplsLdpSessionDown
jnxMplsLdpSessionUp
jnxOspfV3IfConfigError
jnxOspfV3IfRxBadPacket
jnxOspfV3IfStateChange
jnxOspfV3LsdbApproachingOverflow
jnxOspfV3LsdbOverflow
jnxOspfV3NbrRestartHelperStatusChange

jnxOspfV3NbrStateChange
jnxOspfV3NssaTranslatorStatusChange
jnxOspfV3RestartStatusChange
jnxOspfV3VirtIfConfigError
jnxOspfV3VirtIfRxBadPacket
jnxOspfV3VirtIfStateChange
jnxOspfV3VirtNbrRestartHelperStatusChange
jnxOspfV3VirtNbrStateChange
jnxOtnAlarmCleared
jnxOtnAlarmSet
jnxOverTemperature
jnxPMonOverloadCleared
jnxPMonOverloadSet
jnxPingEgressJitterThresholdExceeded
jnxPingEgressStdDevThresholdExceeded
jnxPingEgressThresholdExceeded
jnxPingIngressJitterThresholdExceeded
jnxPingIngressStdDevThresholdExceeded
jnxPingIngressThresholdExceeded
jnxPingRttJitterThresholdExceeded
jnxPingRttStdDevThresholdExceeded
jnxPingRttThresholdExceeded
jnxPortBpduErrorStatusChangeTrap
jnxPortLoopProtectStateChangeTrap
jnxPortRootProtectStateChangeTrap
jnxPowerSupplyFailure
jnxPowerSupplyOK
jnxRedundancySwitchover
jnxRmonAlarmGetFailure
jnxRmonGetOk
jnxSecAccessIfMacLimitExceeded
jnxSecAccessSdsRateLimitCrossed
jnxSonetAlarmCleared
jnxSonetAlarmSet
jnxSpSvcSetCpuExceeded
jnxSpSvcSetCpuOk
jnxSpSvcSetZoneEntered
jnxSpSvcSetZoneExited
jnxStormEventNotification
jnxSyslogTrap
jnxTemperatureOK
jnxVccpPortDown
jnxVccpPortUp
jnxVpnIfDown
jnxVpnIfUp
jnxVpnPwDown
jnxVpnPwUp
jnx12aldGlobalMacLimit
jnx12aldInterfaceMacLimit
jnx12aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange
mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp

```

mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecIllglLb1ThrshExcd
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
sd1cLSStatusChange
sd1cPortStatusChange
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

```

```
ads1AtucRateChangeTrap
ads1AturPerfESsThreshTrap
ads1AturPerfLofsThreshTrap
ads1AturPerfLossThreshTrap
ads1AturPerfLprsThreshTrap
ads1AturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlsWTrapCircuitDown
dlsWTrapCircuitUp
---(more 10%)---
```

show snmp health-monitor

Syntax	show snmp health-monitor <alarms <detail>> <logs>
Release Information	Command introduced in Junos OS Release 8.0. Command introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.
Options	none—Display information about all health monitor alarms and logs. alarms <detail>—(Optional) Display detailed information about health monitor alarms. logs—(Optional) Display information about health monitor logs.
Required Privilege Level	view
List of Sample Output	show snmp health-monitor on page 175 show snmp health-monitor alarms detail on page 177
Output Fields	Table 9 on page 173 describes the output fields for the show snmp health-monitor command. Output fields are listed in the approximate order in which they appear.

Table 9: show snmp health-monitor Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
Variable description	Description of the health monitor object instance being monitored.	All levels
Variable name	Name of the health monitor object instance being monitored.	All levels
Value	Current value of the monitored variable in the most recent sample interval.	All levels

Table 9: show snmp health-monitor Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	<p>State of the alarm or event entry:</p> <ul style="list-style-type: none"> Alarms: <ul style="list-style-type: none"> active—Entry is fully configured and activated. falling threshold crossed—Value of the variable has crossed the lower threshold limit. rising threshold crossed—Value of the variable has crossed the upper threshold limit. under creation—Entry is being configured and is not yet activated. startup—Alarm is waiting for the first sample of the monitored variable. object not available—Monitored variable of that type is not available to the health monitor agent. instance not available—Monitored variable's instance is not available to the health monitor agent. object type invalid—Monitored variable is not a numeric value. object processing errored—An error occurred when the monitored variable was processed. unknown—State is not one of the above. 	All levels
Variable OID	Object ID to which the variable name is resolved. The format is x.x.x.x.	detail
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of absolute value or delta value .	detail
Startup alarm	<p>Alarm that might be sent when this entry is first activated, depending on the following criteria:</p> <ul style="list-style-type: none"> Alarm is sent when one of the following situations exists: <ul style="list-style-type: none"> Value of the alarm is above or equal to the rising threshold and the startup type is either rising alarm or rising or falling alarm. Value of the alarm is below or equal to the falling threshold and the startup type is either falling alarm or rising or falling alarm. Alarm is <i>not</i> sent when one of the following situations exists: <ul style="list-style-type: none"> Value of the alarm is above or equal to the rising threshold and the startup type is falling alarm. Value of the alarm is below or equal to the falling threshold and the startup type is rising alarm. Value of the alarm is between the thresholds. 	detail
Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has monitor prepended to it.	detail
Creator	Mechanism by which the entry was configured (Health Monitor).	detail
Sample interval	Time period between samples (in seconds).	detail
Rising threshold	Upper limit threshold value as a percentage of the maximum possible value.	detail

Table 9: 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 user@host> show snmp health-monitor
health-monitor
Alarm
Index  Variable description          Value State
-----
32768  Health Monitor: root file system utilization
      jnxHrStoragePercentUsed.1      58 active
32769  Health Monitor: /config file system utilization
      jnxHrStoragePercentUsed.2      0 active
32770  Health Monitor: RE 0 CPU utilization
      jnxOperatingCPU.9.1.0.0        0 active
32773  Health Monitor: RE 0 Memory utilization
      jnxOperatingBuffer.9.1.0.0     35 active
32775  Health Monitor: jkernel daemon CPU utilization
      Init daemon                    0 active
      Chassis daemon                 50 active
      Firewall daemon                 0 active
      Interface daemon                5 active
      SNMP daemon                     11 active
      MIB2 daemon                     42 active
      Sonet APS daemon                0 active
      VRRP daemon                     0 active
      Alarm daemon                    3 active
      PFE daemon                      0 active
      CRAFT daemon                    0 active
      Traffic sampling control daemon 0 active
      Ilmi daemon                     0 active
      Remote operations daemon         0 active
      CoS daemon                      0 active
      Pic Services Logging daemon      0 active
      Internal Routing Service Daemon  3 active
      Network Access Service daemon    0 active
      Forwarding UDP daemon            0 active
      Routing socket proxy daemon      0 active
      Disk Monitoring daemon           1 active
      Inet daemon                     0 active
      Syslog daemon                   0 active
      Adaptive Services PIC daemon     0 active
      ECC parity errors logging Daemon 0 active
      Layer 2 Tunneling Protocol daemon 0 active
      PPPoE daemon                     3 active
      Redundancy device daemon         0 active

```

PPP daemon	0 active
Dynamic Flow Capture Daemon	0 active
32776 Health Monitor: jroute daemon CPU utilization	
Routing protocol daemon	1 active
Management daemon	0 active
Management daemon	0 active
Command line interface	4 active
Periodic Packet Management daemon	0 active
Link Management daemon	0 active
Pragmatic General Multicast daemon	0 active
Bidirectional Forwarding Detection daemon	0 active
SRC daemon	0 active
audit daemon	0 active
Event daemon	0 active
32777 Health Monitor: jcrypto daemon CPU utilization	
IPSec Key Management daemon	0 active
32779 Health Monitor: jkernel daemon Memory utilization	
Init daemon	47384 active
Chassis daemon	20204 active
Firewall daemon	1956 active
Interface daemon	3340 active
SNMP daemon	4540 active
MIB2 daemon	3880 active
Sonet APS daemon	2632 active
VRRP daemon	2672 active
Alarm daemon	1856 active
PFE daemon	2600 active
CRAFT daemon	2000 active
Traffic sampling control daemon	3164 active
Ilmi daemon	2132 active
Remote operations daemon	2964 active
CoS daemon	3044 active
Pic Services Logging daemon	1944 active
Internal Routing Service Daemon	1392 active
Network Access Service daemon	1992 active
Forwarding UDP daemon	1876 active
Routing socket proxy daemon	1296 active
Disk Monitoring daemon	1180 active
Inet daemon	1296 active
Syslog daemon	1180 active
Adaptive Services PIC daemon	3220 active
ECC parity errors logging Daemon	1100 active
Layer 2 Tunneling Protocol daemon	3372 active
PPPoE daemon	1424 active
Redundancy device daemon	1820 active
PPP daemon	2060 active
Dynamic Flow Capture Daemon	10740 active
32780 Health Monitor: jroute daemon Memory utilization	
Routing protocol daemon	8104 active
Management daemon	13360 active
Management daemon	19252 active
Command line interface	9912 active
Periodic Packet Management daemon	1484 active
Link Management daemon	2016 active
Pragmatic General Multicast daemon	1968 active
Bidirectional Forwarding Detection daemon	1956 active
SRC daemon	1772 active
audit daemon	1772 active

Event daemon 1808 active

32781 Health Monitor: jcrypto daemon Memory utilization
IPSec Key Management daemon 5600 active

show snmp
health-monitor alarms
detail

user@host> show snmp health-monitor alarms detail

```
Alarm Index 32768:
Variable name          jnxHrStoragePercentUsed.1
Variable OID           1.3.6.1.4.1.2636.3.31.1.1.1.1.1
Sample type            absolute value
Startup alarm          rising alarm
Owner                  Health Monitor: root file system
                       utilization
Creator                Health Monitor
State                  active
Sample interval        300 seconds
Rising threshold       80
Falling threshold      70
Rising event index     32768
Falling event index    32768
Instance Value: 58
Instance State: active

Alarm Index 32769:
Variable name          jnxHrStoragePercentUsed.2
Variable OID           1.3.6.1.4.1.2636.3.31.1.1.1.1.2
Sample type            absolute value
Startup alarm          rising alarm
Owner                  Health Monitor: /config file system
                       utilization
Creator                Health Monitor
State                  active
Sample interval        300 seconds
Rising threshold       80
Falling threshold      70
Rising event index     32768
Falling event index    32768
Instance Value: 0
Instance State: active

Alarm Index 32770:
Variable name          jnxOperatingCPU.9.1.0.0
Variable OID           1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
Sample type            absolute value
Startup alarm          rising alarm
Owner                  Health Monitor: RE 0 CPU utilization

Creator                Health Monitor
State                  active
Sample interval        300 seconds
Rising threshold       80
Falling threshold      70
Rising event index     32768
Falling event index    32768
Instance Value: 0
Instance State: active

Alarm Index 32773:
Variable name          jnxOperatingBuffer.9.1.0.0
```

Variable OID 1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: RE 0 Memory utilization

Creator Health Monitor
State active
Sample interval 300 seconds
Rising threshold 80
Falling threshold 70
Rising event index 32768
Falling event index 32768
Instance Value: 35
Instance State: active

Alarm Index 32775:

Variable name sysAppElmtRunCPU.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: sysAppElmtRunCPU.3.1.1
Instance Description: Init daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElmtRunCPU.3.2.2786
Instance Description: Chassis daemon
Instance Value: 50
Instance State: active

Instance Name: sysAppElmtRunCPU.3.3.2938
Instance Description: Firewall daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElmtRunCPU.3.4.2942
Instance Description: Interface daemon
Instance Value: 5
Instance State: active

Instance Name: sysAppElmtRunCPU.3.7.7332
Instance Description: SNMP daemon
Instance Value: 11
Instance State: active

Instance Name: sysAppElmtRunCPU.3.9.2914
Instance Description: MIB2 daemon
Instance Value: 42
Instance State: active

Instance Name: sysAppElmtRunCPU.3.12.2916

Instance Description: Sonet APS daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.13.2917
Instance Description: VRRP daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.14.2787
Instance Description: Alarm daemon
Instance Value: 3
Instance State: active

Instance Name: sysAppElemRunCPU.3.15.2940
Instance Description: PFE daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.16.2788
Instance Description: CRAFT daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.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.
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 180
Output Fields	Table 10 on page 180 describes the output fields for the show snmp inform-statistics command. Output fields are listed in the approximate order in which they appear.

Table 10: 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
Target Name: TA2_v3_sha_none Address: 192.168.110.59
Sent: 0, Pending: 4
Discarded: 84, Timeouts: 0, Probe Failures: 258

```

Target Name: TA5_v2_none Address: 172.17.20.184
Sent: 0, Pending: 0
Discarded: 2, Timeouts: 10, Probe Failures: 0

show snmp 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 184 show snmp rmon alarms detail on page 184 show snmp rmon events detail on page 185
Output Fields	Table 11 on page 182 describes the output fields for the show snmp rmon command. Output fields are listed in the approximate order in which they appear.

Table 11: show snmp rmon Output Fields

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

Table 11: show snmp rmon Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	<p>State of the alarm or event entry:</p> <p>Alarms:</p> <ul style="list-style-type: none"> • active—Entry is fully configured and activated. • falling threshold crossed—Value of the variable has crossed the lower threshold limit. • rising threshold crossed—Value of the variable has crossed the upper threshold limit. • under creation—Entry is being configured and is not yet activated. • startup—Alarm is waiting for the first sample of the monitored variable. • object not available—Monitored variable of that type is not available to the SNMP agent. • instance not available—Monitored variable's instance is not available to the SNMP agent. • object type invalid—Monitored variable is not a numeric value. • object processing errored—An error occurred when the monitored variable was processed. • unknown—State is not one of the above. <p>Events:</p> <ul style="list-style-type: none"> • active—Entry has been fully configured and activated. • under creation—Entry is being configured and is not yet activated. • unknown—State is not one of the above. 	All levels
Variable name	Name of the SNMP object instance being monitored.	All levels
Event Index	Event identifier.	All levels
Type	<p>Type of notification made when an event is triggered. It can be one of the following:</p> <ul style="list-style-type: none"> • log—A system log message is generated and an entry is made to the log table. • snmptrap—An SNMP trap is sent to the configured destination. • log and trap—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination. • none—Neither log nor trap will be sent. 	detail
Last Event	Date and time of the last event. It has the format <i>yyyy-mm-dd hh:mm:ss timezone</i> .	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

Table 11: 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: <ul style="list-style-type: none"> Alarm is sent when one of the following situations exists: <ul style="list-style-type: none"> Value of the alarm is above or equal to the rising threshold and the startup type is either rising alarm or rising or falling alarm. Value of the alarm is below or equal to the falling threshold and the startup type is either falling alarm or rising or falling alarm. Alarm is <i>not</i> sent when one of the following situations exists: <ul style="list-style-type: none"> Value of the alarm is above or equal to the rising threshold and the startup type is falling alarm. Value of the alarm is below or equal to the falling threshold and the startup type is rising alarm. Value of the alarm is between the thresholds. 	detail
Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has monitor prepended to it.	detail
Creator	Mechanism by which the entry was configured (CLI or SNMP).	detail
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 user@host> show snmp rmon alarms detail
alarms detail
Alarm Index 1:
Variable name      ifInOctets.1
Variable OID       1.3.6.1.2.1.2.2.1.10.1

```


Sample type		delta value
Startup alarm		rising or falling alarm
Owner		monitor
Creator		CLI
State		falling threshold crossed
Sample interval	60	seconds
Rising threshold	100000	
Falling threshold	80000	
Rising event index	1	
Falling event index	1	
Current value	0	

```
show snmp rmon events detail user@host> show snmp rmon events detail
Event Index 1:
  Type          log and trap
  Community     boy-elroy
  Last event    2002-01-30 01:13:01 PST
  Creator       CLI
  State         active
```

show snmp rmon history

Syntax	show snmp rmon history <i><history-index></i> <i><sample-index></i>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display the contents of the RMON history group.
Options	<p>none—Display all the entries in the RMON history group.</p> <p><i>history-index</i>—(Optional) Display the contents of the specified entry in the RMON history group.</p> <p><i>sample-index</i>—(Optional) Display the statistics collected for the specified sample within the specified entry in the RMON history group.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear snmp rmon history on page 164
List of Sample Output	show snmp rmon history 1 on page 187 show snmp rmon history 1 sample 15 on page 188
Output Fields	<p>Table 12 on page 186 lists the output fields for the show smp rmon history command. Output fields are listed in the approximate order in which they appear.</p>

Table 12: 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 ifindex object that identifies the interface that is being monitored.
Interval	The interval (in seconds) configured for this RMON history entry.
Buckets Requested	The requested number of buckets (intervals) configured for this RMON history entry.
Buckets Granted	The number of buckets granted for this RMON history entry.

Table 12: show smp rmon history Output Fields (*continued*)

Field Name	Field Description
Sample Index	<p>The sample statistics taken at the specified interval.</p> <ul style="list-style-type: none"> • Drop Events—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Octets—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. • Packets—Total number of packets. • Broadcast Packets—Number of broadcast packets. • Multicast Packets—Number of multicast packets. • CRC errors—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error). • Undersize Pkts—Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. • Oversize Pkts—Number of packets received during the sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets) but were otherwise well formed. • Fragments—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted. • Jabbers—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms. • Collisions—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug. • Utilization(%)—The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Sample Output

```

show snmp rmon history 1
user@host> show snmp rmon history 1
History Index 1:
Interface                               171
Requested Buckets                        50
Interval                                10

Sample Index 1: Interval Start: Tue Feb 12 04:12:32 2008
Drop Events                             0
Octets                                  486
Packets                                 2
Broadcast Packet                         0
Multicast Packets                        2

```

```

CRC errors          0
Undersize Pkts      0
Oversize Pkts       0
Fragments           0
Jabbers             0
Collisions           0
Utilization(%)      0

```

Sample Index 2: Interval Start: Tue Feb 12 04:12:42 2008

```

Drop Events         0
Octets              486
Packets             2
Broadcast Packet    0
Multicast Packets   2
CRC errors          0
Undersize Pkts      0
Oversize Pkts       0
Fragments           0
Jabbers             0
Collisions           0
Utilization(%)      0

```

Sample Index 3: Interval Start: Tue Feb 12 04:12:52 2008

```

Drop Events         0
Octets              486
Packets             2
Broadcast Packet    0
Multicast Packets   2
CRC errors          0
Undersize Pkts      0
Oversize Pkts       0
Fragments           0
Jabbers             0
Collisions           0
Utilization(%)      0

```

**show snmp rmon
history 1 sample 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
Octets      = 0
Packets     = 0
Broadcast Pkts = 0
Multicast Pkts = 0
CRC Errors  = 0
Undersize Pkts = 0
Oversize Pkts = 0
Fragments   = 0
Jabbers     = 0
Collisions  = 0

```

Utilization (%) = 0

show snmp statistics

Syntax	show snmp statistics
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear snmp statistics on page 165
List of Sample Output	show snmp statistics on page 193
Output Fields	Table 13 on page 190 describes the output fields for the show snmp statistics command. Output fields are listed in the approximate order in which they appear.

Table 13: show snmp statistics Output Fields

Field Name	Field Description
Input	<p>Information about received packets:</p> <ul style="list-style-type: none"> Packets(snmplnPkts)—Total number of messages delivered to the SNMP entity from the transport service. Bad versions—(snmplnBadVersions) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. Bad community names—(snmplnBadCommunityNames) Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. Bad community uses—(snmplnBadCommunityUses) Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. ASN parse errors—(snmplnASNParseErrs) Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. Too big—(snmplnTooBig) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of tooBig. No such names—(snmplnNoSuchNames) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of noSuchName. Bad values—(snmplnBadValues) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of badValue. Read only—(snmplnReadOnly) Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of readOnly. Only incorrect implementations of SNMP generate this error.

Table 13: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
Input (continued)	<ul style="list-style-type: none"> • General errors—(snmpInGenErrs) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of genErr. • Total requests varbinds—(snmpInTotalReqVars) Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP GetRequest and GetNext PDUs. • Total set varbinds—(snmpInSetVars) Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP SetRequest PDUs. • Get requests—(snmpInGetRequests) Total number of SNMP GetRequest PDUs that have been accepted and processed by the SNMP entity. • Get nexts—(snmpInGetNexts) Total number of SNMP GetNext PDUs that have been accepted and processed by the SNMP entity. • Set requests—(snmpInSetRequests) Total number of SNMP SetRequest PDUs that have been accepted and processed by the SNMP entity. • Get responses—(snmpInGetResponses) Total number of SNMP GetResponse PDUs that have been accepted and processed by the SNMP entity. • Traps—(snmpInTraps) Total number of SNMP traps generated by the SNMP entity. • Silent drops—(snmpSilentDrops) Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • Proxy drops—(snmpProxyDrops) Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • Commit pending drops—Number of SNMP packets for Set requests dropped because of a previous pending SNMP Set request on the committed configuration. • Throttle drops—Number of SNMP packets for any requests dropped reaching the throttle limit.

Table 13: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
V3 Input	<p>Information about SNMP version 3 packets:</p> <ul style="list-style-type: none"> • Unknown security models—(snmpUnknownSecurityModels) Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • Invalid messages—(snmpInvalidMsgs) Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • Unknown pdu handlers—(snmpUnknownPDUHandlers) Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • Unavailable contexts—(snmpUnavailableContexts) Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • Unknown contexts—(snmpUnknownContexts) Total number of requests received for a context that is unknown to the SNMP engine. • Unsupported security levels—(usmStatsUnsupportedSecLevels) Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • Not in time windows—(usmStatsNotInTimeWindows) Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • Unknown user names—(usmStatsUnknownUserNames) Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • Unknown engine ids—(usmStatsUnknownEngineIDs) Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • Wrong digests—(usmStatsWrongDigests) Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • Decryption errors—(usmStatsDecryptionErrors) Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 13: show snmp statistics Output Fields (*continued*)

Field Name	Field Description
Output	<p>Information about transmitted packets:</p> <ul style="list-style-type: none"> • Packets—(snmpOutPkts) Total number of messages passed from the SNMP entity to the transport service. • Too big—(snmpOutTooBig) Total number of SNMP PDUs generated by the SNMP entity with an error status field of tooBig. • No such names—(snmpOutNoSuchNames) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of noSuchName. • Bad values—(snmpOutBadValues) Total number of SNMP PDUs generated by the SNMP entity with an error status field of badValue. • General errors—(snmpOutGenErrs) Total number of SNMP PDUs generated by the SNMP entity with an error status field of genErr. • Get requests—(snmpOutGetRequests) Total number of SNMP GetRequest PDUs generated by the SNMP entity. • Get nexts—(snmpOutGetNexts) Total number of SNMP GetNext PDUs generated by the SNMP entity. • Set requests—(snmpOutSetRequests) Total number of SNMP SetRequest PDUs generated by the SNMP entity. • Get responses—(snmpOutGetResponses) Total number of SNMP GetResponse PDUs generated by the SNMP entity. • Traps—(snmpOutTraps) Total number of SNMP traps generated by the SNMP entity.

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 big: 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 big: 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 v3

Syntax	<code>show snmp v3</code> <code><access <brief detail> community general groups notify <filter> target <address parameters> users></code>
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	<code>none</code> —Display all of the SNMPv3 operating configuration. <code>access</code> —(Optional) Display SNMPv3 access information. <code>brief detail</code> —(Optional) Display brief or detailed information about SNMPv3 access information. <code>community</code> —(Optional) Display SNMPv3 community information. <code>general</code> —(Optional) Display SNMPv3 general information. <code>groups</code> —(Optional) Display SNMPv3 security-to-group information. <code>notify <filter></code> —(Optional) Display SNMPv3 notify and, optionally, notify filter information. <code>target <address parameters></code> —(Optional) Display SNMPv3 target and, optionally, either target address or target parameter information. <code>users</code> —(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 196
Output Fields	Table 14 on page 195 describes the output fields for the show snmp v3 command. Output fields are listed in the approximate order in which they appear.

Table 14: show snmp v3 Output Fields

Field Name	Field Description
Access control	<p>Information about access control:</p> <ul style="list-style-type: none"> • Group—Group name for which the configured access privileges apply. The group, together with the context prefix and the security model and security level, forms the index for this table. • Context prefix—SNMPv3 context for which the configured access privileges apply. • Security model/level—Security model and security level for which the configuration access privileges apply. • Read view—Identifies the MIB view applied to SNMPv3 read operations. • Write view—Identifies the MIB view applied to SNMPv3 write operations. • Notify view—Identifies the MIB view applied to outbound SNMP notifications.
Engine	<p>Information about local engine configuration:</p> <ul style="list-style-type: none"> • Local engine ID—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • Engine boots—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • Engine time—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • Max msg size—Maximum message size the sender can accommodate.
Engine ID	<p>Information about engine ID:</p> <ul style="list-style-type: none"> • Local engine ID—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine. • Engine boots—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed. • Engine time—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • Max msg size—Maximum message size the sender can accommodate. • Engine ID—SNMPv3 engine ID associated with each user. • User—SNMPv3 user. • Auth/Priv—Authentication and encryption algorithm available for use by each user. • Storage—Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status. • Status—Status of the conceptual row. Only rows with an active status are used by the SNMPv3 engine.
Group name	Name of the group to which this entry belongs.
Security model	Identifies the security model context for the security name.
Security name	Used with the security model; identifies a specific security name instance. Each security model/security name combination can be assigned to a specific group.
Storage type	Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.
Status	Status of the conceptual row. Only rows with active status are used by the SNMPv3 engine.

Sample Output

```

show snmp v3 user@host> show snmp v3
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots:      38
Engine time:       64583 seconds
Max msg size:      2048 bytes

Engine ID: local
  User          Auth/Priv  Storage  Status
  user1         md5/des   nonvolatile active
  user2         sha/none nonvolatile active
  user3         none/none nonvolatile active

Engine ID: 81 00 0a 4c 04 64 64 64 64
  User          Auth/Priv  Storage  Status
  UNEW         md5/none  nonvolatile active
Group name      Security  Security  Storage  Status
                model    name      type
g1              usm      user1     nonvolatile active
g2              usm      user2     nonvolatile active
g3              usm      user3     nonvolatile active

Access control:
Group           Context  Security  Read    Write    Notify
                prefix  model/level view     view     view
g1              usm/privacy v1       v1
g2              usm/authent v1       v1
g3              usm/none    v1       v1
  
```

CHAPTER 4

Real-Time Performance Monitoring (RPM)

- [RPM—Overview on page 197](#)
- [Configuring Real-Time Performance Monitoring \(RPM\) on page 201](#)
- [Verifying Real-Time Performance Monitoring on page 210](#)
- [Configuration Statements for Real-Time Performance Monitoring on page 211](#)
- [Operational Commands for Real-Time Performance Monitoring on page 229](#)

RPM—Overview

- [Understanding Real-Time Performance Monitoring on EX Series Switches on page 198](#)

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 198](#)
- [Tests and Probe Types on page 198](#)
- [Hardware Timestamps on page 199](#)
- [Limitations of RPM on EX Series Switches on page 201](#)

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:
 - 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

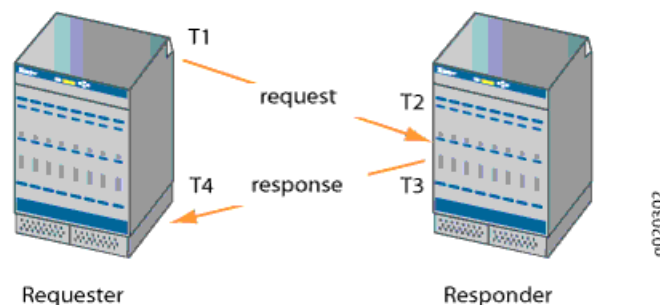
You should configure the requester (the RPM client) with hardware timestamps (see [Figure 6 on page 200](#)) to get more meaningful results than you would get without the timestamps. The responder (the RPM server) does not need to be configured to support hardware timestamps. If the responder supports 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 6 on page 200](#) shows the timestamps:

Figure 6: 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 208](#) 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 6 on page 200](#), one-way timestamps represent the time $T2 - T1$ and the time from $T4 - T3$. Use one-way timestamps when you want to gather information about delay in each direction and to find egress and ingress jitter values.



NOTE: For correct one-way measurement, the clocks of the requester and responder must be synchronized. If the clocks are not synchronized, one-way jitter measurements and calculations can include significant variations, in some cases orders of magnitude greater than the round-trip times.

When you enable one-way timestamps in a probe, the following one-way measurements are reported:

- Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times
- Number of probes sent
- Number of probe responses received
- Percentage of lost probes

Limitations of RPM on EX Series 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 208](#)
- [Configuring Real-Time Performance Monitoring \(J-Web Procedure\) on page 201](#)
- [Configuring SNMP \(J-Web Procedure\) on page 95](#)
- [Monitoring Network Traffic Using Traceroute on page 341](#)

Configuring Real-Time Performance Monitoring (RPM)

- [Configuring Real-Time Performance Monitoring \(J-Web Procedure\) on page 201](#)
- [Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch \(CLI Procedure\) on page 208](#)

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

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:

- 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 should 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.

**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 15 on page 203](#).
 - 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 15: 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.	<ol style="list-style-type: none"> 1. Click Add and type an owner name. 2. In Performance Probe Tests, click Add to define the RPM test parameters. See Table 16 on page 204 for information on configuring RPM test parameters. 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.

Table 15: 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.	<p>Set up the following servers:</p> <ul style="list-style-type: none"> 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. 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 16: 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		

Table 16: 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: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping • 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. 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.

Table 16: 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.

Table 16: 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.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates SNMP traps when the threshold for maximum inbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates SNMP traps when the threshold for jitter in round-trip time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.

Table 16: 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.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
RTT Exceeded	Generates SNMP traps when the threshold for maximum round-trip time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. 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.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Test Completion	Generates SNMP traps when a test is completed.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. 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.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.

- Related Documentation**
- [Configuring SNMP \(J-Web Procedure\) on page 95](#)
 - [Viewing Real-Time Performance Monitoring Information on page 210](#)

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:

- **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 201](#)
- [Understanding Real-Time Performance Monitoring on EX Series Switches on page 198](#)

Verifying Real-Time Performance Monitoring

- [Viewing Real-Time Performance Monitoring Information on page 210](#)

Viewing Real-Time Performance Monitoring Information

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 201](#)

Configuration Statements for Real-Time Performance Monitoring

data-fill

Syntax	<code>data-fill data;</code>
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.
Description	Specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes.
Options	data —A hexadecimal value; for example, 0-9 , A-F .
Usage Guidelines	The data-fill statement is not valid with the http-get or http-metadata-get probe types. See Configuring BGP Neighbor Discovery Through RPM or Configuring Real-Time Performance Monitoring.
Required Privilege Level	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.

data-size

Syntax	<code>data-size size;</code>
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.
Description	Specify the size of the data portion of ICMP probes.
Options	data —The size can be from 0 through 65507 Default: 0
<div><p>NOTE: If you configure the hardware timestamp feature (see Configuring Real-Time Performance Monitoring), the <code>data-size</code> default value 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.</p></div>	
Usage Guidelines	The <code>data-size</code> statement is not valid with the <code>http-get</code> or <code>http-metadata-get</code> probe type. See Configuring BGP Neighbor Discovery Through RPM or Configuring Real-Time Performance Monitoring.
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.

destination-port

Syntax	<code>destination-port <i>port</i>;</code>
Hierarchy Level	[edit services rpm bgp], [edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
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.
Options	port —The port number can be 7 or from 49,160 to 65,535.
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring Real-Time Performance Monitoring.
Required Privilege Level	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.

dscp-code-point

Syntax	<code>dscp-code-point <i>dscp-bits</i>;</code>
Hierarchy Level	[edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
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	<p><i>dscp-bits</i>—A valid 6-bit pattern; for example, 001111, or one of the following configured DSCP aliases:</p> <ul style="list-style-type: none">• af11—Default: 001010• af12—Default: 001100• af13—Default: 001110• af21—Default: 010010• af22—Default: 010100• af23 —Default: 010110• af31 —Default: 011010• af32 —Default: 011100• af33 —Default: 011110• af41 —Default: 100010• af42 —Default:100100• af43 —Default:100110• be—Default: 000000• cs1—Default: 001000• cs2—Default: 010000• cs3—Default: 011000• cs4—Default: 100000• cs5—Default: 101000• cs6—Default: 110000• cs7—Default: 111000• ef—Default: 101110• nc1—Default: 110000• nc2—Default: 111000

Usage Guidelines	See Configuring Real-Time Performance Monitoring.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

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	On MX Series routers and EX Series switches only, 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.
Usage Guidelines	See Configuring RPM Timestamping.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

history-size

Syntax	history-size <i>size</i> ;
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.
Description	Specify the number of stored history entries.
Options	size —A value from 0 to 255. Default: 50
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring RPM Probes.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

moving-average-size

Syntax	<code>moving-average-size <i>number</i>;</code>
Hierarchy Level	[edit services rpm bgp], [edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Enable statistical calculation operations to be performed across a configurable number of the most recent samples.
Options	<i>number</i> —Number of samples to be used in calculations. Range: 0 through 255
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

one-way-hardware-timestamp

Syntax	<code>one-way-hardware-timestamp;</code>
Hierarchy Level	[edit services rpm probe owner test <i>test-name</i>]
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.
Usage Guidelines	See Configuring RPM Timestamping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">destination-interface, hardware-timestamp on page 215

port (RPM)

Syntax	<code>port <i>number</i>;</code>
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.
Description	Specify the port number for the probe server.
Options	<i>number</i> —Port number for the probe server. The value can be 7 or 49,160 through 65,535.
Usage Guidelines	See Configuring RPM Receiver Servers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

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;  
            moving-average-size number;  
            one-way-hardware-timestamp;  
            probe-count count;  
            probe-interval seconds;  
            probe-type type;  
            routing-instance instance-name;  
            source-address address;  
            target (url | address);  
            test-interval interval;  
            thresholds thresholds;  
            traps traps;  
        }  
    }
```

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*—Specify an owner name up to 32 characters in length.

The remaining statements are explained separately.

Usage Guidelines See Configuring RPM Probes.

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

probe-count

Syntax	<code>probe-count <i>count</i>;</code>
Hierarchy Level	[edit services rpm bgp], [edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the number of probes within a test.
Options	count —A value from 1 through 15.
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

probe-interval

Syntax	<code>probe-interval <i>interval</i>;</code>
Hierarchy Level	[edit services rpm bgp], [edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the time to wait between sending packets, in seconds.
Options	interval —Number of seconds, from 1 through 255.
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

probe-limit

Syntax	<code>probe-limit <i>limit</i>;</code>
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 the maximum number of concurrent probes allowed.
Options	<i>limit</i> —A value from 1 through 500. Default: 100.
Usage Guidelines	See Limiting the Number of Concurrent RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

probe-server

Syntax	<pre>probe-server { tcp { destination-interface <i>interface-name</i>; port <i>number</i>; } udp { destination-interface <i>interface-name</i>; port <i>number</i>; } }</pre>
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 the server to act as a receiver for the probes. The remaining statements are explained separately.
Usage Guidelines	See Configuring RPM Receiver Servers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

probe-type

Syntax	<code>probe-type type;</code>
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.
Description	Specify the packet and protocol contents of a probe.
Options	<p>type—Specify one of the following probe type values:</p> <ul style="list-style-type: none"> • 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.
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring RPM Probes.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

routing-instance

Syntax	<code>routing-instance <i>instance-name</i>;</code>
Hierarchy Level	<code>[edit services rpm <i>probe owner test test-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the routing instance used by the probes.
Options	<i>instance-name</i> —A routing instance configured at the <code>[edit routing-instance]</code> hierarchy level. Default: Internet routing table <code>inet.0</code> .
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

routing-instances

Syntax	<code>routing-instances <i>instance-name</i>;</code>
Hierarchy Level	<code>[edit services rpm bgp],</code> <code>[edit services rpm bgp logical-system <i>logical-system-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the routing instance used by the probes.
Options	<i>instance-name</i> —A routing instance configured at the <code>[edit routing-instances]</code> hierarchy level. Default: Internet routing table <code>inet.0</code> .
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

rpm

Syntax	<code>rpm (client server);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 8.1. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Associate an RPM client (router or switch that originates RPM probes) or RPM server with a specified interface.
Options	<i>client</i> —Identifier for RPM client router or switch. <i>server</i> —Identifier for RPM server.
Usage Guidelines	See Configuring RPM Timestamping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address

Syntax	<code>source-address <i>address</i>;</code>
Hierarchy Level	[edit services rpm <i>probe owner test test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
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 will use the outgoing interface's address as its source.
Options	<i>address</i> —Valid IP address.
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

target

Syntax	<code>target (url <i>url</i> address <i>address</i>);</code>
Hierarchy Level	[edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the destination address used for the probes.
Options	url <i>url</i> —For HTTP probe types, specify a fully formed URL that includes http:// in the URL address. address <i>address</i> —For all other probe types, specify an IPv4 address for the target host.
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

tcp

Syntax	<pre>tcp { destination-interface <i>interface-name</i>; port <i>port</i>; }</pre>
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.
Description	Specify the port information for the TCP server. The remaining statements are explained separately.
Usage Guidelines	See Configuring RPM Receiver Servers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

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;`
 `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.

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**—Specify a test name. The name can be up to 32 characters in length.
 The remaining statements are explained separately.

Usage Guidelines See Configuring RPM Probes.

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

test-interval

Syntax	<code>test-interval <i>frequency</i>;</code>
Hierarchy Level	[edit services rpm bgp], [edit services rpm probe owner test <i>test-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the time to wait between tests, in seconds.
Options	<i>frequency</i> —Number of seconds, from 0 through 86400.
Usage Guidelines	See Configuring BGP Neighbor Discovery Through RPM or Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

thresholds

Syntax	<code>thresholds thresholds;</code>
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.
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.
Options	<p>thresholds—Specify one or more threshold measurements. The following options are supported:</p> <ul style="list-style-type: none"> • 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.
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

traps

Syntax	<code>traps traps;</code>
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.
Description	Set the trap bit to generate traps for probes. Traps are sent if the configured threshold is met or exceeded.
Options	<p>traps—Specify one or more traps. The following options are supported:</p> <ul style="list-style-type: none">• egress-jitter-exceeded—Generates traps when the jitter in egress time threshold is met or exceeded.• egress-std-dev-exceeded—Generates traps when the egress time standard deviation threshold is met or exceeded.• egress-time-exceeded—Generates traps when the maximum egress time threshold is met or exceeded.• ingress-jitter-exceeded—Generates traps when the jitter in ingress time threshold is met or exceeded.• ingress-std-dev-exceeded—Generates traps when the ingress time standard deviation threshold is met or exceeded.• ingress-time-exceeded—Generates traps when the maximum ingress time threshold is met or exceeded.• jitter-exceeded—Generates traps when the jitter in round-trip time threshold is met or exceeded.• probe-failure—Generates traps for successive probe loss thresholds crossed.• rtt-exceeded—Generates traps when the maximum round-trip time threshold is met or exceeded.• std-dev-exceeded—Generates traps when the round-trip time standard deviation threshold is met or exceeded.• test-completion—Generates traps when a test is completed.• test-failure—Generates traps when the total probe loss threshold is met or exceeded.
Usage Guidelines	See Configuring RPM Probes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

udp

Syntax	<pre>udp { destination-interface <i>interface-name</i>; port <i>port</i>; }</pre>
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.
Description	Specify the port information for the UDP server. The remaining statements are explained separately.
Usage Guidelines	See Configuring RPM Receiver Servers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

Operational Commands for Real-Time Performance Monitoring

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.
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 230
Output Fields	Table 17 on page 230 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	<pre>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</pre>
---	---

show services rpm history-results

Syntax	show services rpm history-results <brief detail> <owner <i>owner</i> > <since <i>time</i> > <test <i>name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) instance.
Options	<p>none—Display the results of the last 50 probes for all RPM instances.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>owner <i>owner</i>—(Optional) Display information for the specified probe owner.</p> <p>since <i>time</i>—(Optional) Display information from the specified time. Specify time as <i>yyyy-mm-dd.hh:mm:ss</i>.</p> <p>test <i>name</i>—(Optional) Display information for the specified test.</p>
Required Privilege Level	view
List of Sample Output	show services rpm history-results on page 232 show services rpm history-results detail on page 232
Output Fields	Table 18 on page 231 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	<p>Result of a particular probe performed by a remote host. The following information is contained in the results:</p> <ul style="list-style-type: none"> Response received—Timestamp when the probe result was determined. Rtt—Average ping round-trip time (RTT), in microseconds. 	detail

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	<p>Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-pin-timestamp, the egress and ingress delay:</p> <ul style="list-style-type: none"> • Minimum—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. • Maximum—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. • Average—Average RTT, ingress delay, or egress delay measured over the course of the current test. • Jitter—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test. • Stddev—Standard deviation of the round-trip time, in microseconds, measured over the course of the current test. 	detail

Sample Output

```

show services rpm history-results user@host> show services rpm history-results
Owner, Test                               Probe received                               Round trip time
flintstone, 0                             Tue Dec 28 15:56:22 2004                       158 usec
flintstone, 0                             Tue Dec 28 15:56:23 2004                       218 usec
flintstone, 0                             Tue Dec 28 15:56:24 2004                       161 usec
flintstone, 0                             Tue Dec 28 15:56:25 2004                       184 usec
flintstone, 0                             Tue Dec 28 15:56:30 2004                       332 usec
flintstone, 0                             Tue Dec 28 15:56:31 2004                       132 usec
flintstone, 0                             Tue Dec 28 15:56:32 2004                       226 usec
flintstone, 0                             Tue Dec 28 15:56:33 2004                       191 usec
flintstone, 0                             Tue Dec 28 15:56:34 2004                       179 usec
flintstone, 0                             Tue Dec 28 15:56:39 2004                       217 usec
flintstone, 0                             Tue Dec 28 15:56:40 2004                       141 usec
flintstone, 0                             Tue Dec 28 15:56:41 2004                       230 usec
flintstone, 0                             Tue Dec 28 15:56:42 2004                       248 usec
flintstone, 0                             Tue Dec 28 15:56:43 2004                       234 usec
flintstone, 0                             Tue Dec 28 15:56:48 2004                       251 usec
flintstone, 0                             Tue Dec 28 15:56:49 2004                       134 usec
flintstone, 0                             Tue Dec 28 15:56:50 2004                       272 usec
flintstone, 0                             Tue Dec 28 15:56:51 2004                       181 usec
flintstone, 0                             Tue Dec 28 15:56:52 2004                       216 usec
flintstone, 0                             Tue Dec 28 15:56:57 2004                       227 usec
flintstone, 0                             Tue Dec 28 15:56:58 2004                       133 usec

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

```



```
Owner: flintstone, Test: 0
Probe results:
  Response received, Tue Dec 28 15:56:39 2004
  Rtt: 217 usec
Results over current test:
  Probes sent: 1, Probes received: 1, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 217 usec, Maximum: 217 usec, Average: 217 usec,
    Jitter: 0 usec, Stddev: 0 usec

Owner: flintstone, Test: 0
Probe results:
  Response received, Tue Dec 28 15:56:40 2004
  Rtt: 141 usec
Results over current test:
  Probes sent: 2, Probes received: 2, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 141 usec, Maximum: 217 usec, Average: 179 usec,
    Jitter: 76 usec, Stddev: 38 usec

Owner: flintstone, Test: 0
Probe results:
  Response received, Tue Dec 28 15:56:41 2004
  Rtt: 230 usec
Results over current test:
  Probes sent: 3, Probes received: 3, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 141 usec, Maximum: 230 usec, Average: 196 usec,
    Jitter: 89 usec, Stddev: 39 usec

Owner: flintstone, Test: 0
Probe results:
  Response received, Tue Dec 28 15:56:42 2004
  Rtt: 248 usec
Results over current test:
  Probes sent: 4, Probes received: 4, Loss percentage: 0
  Measurement: Round trip time
    Minimum: 141 usec, Maximum: 248 usec, Average: 209 usec,
    Jitter: 107 usec, Stddev: 41 usec
```

show services rpm probe-results

Syntax	show services rpm probe-results <owner <i>owner</i> > <test <i>name</i> >
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 results of the most recent real-time performance monitoring (RPM) probes.
Options	none—Display all results of the most recent RPM probes. owner <i>owner</i> —(Optional) Display information for the specified probe owner. test <i>name</i> —(Optional) Display information for the specified test.
Required Privilege Level	view
List of Sample Output	show services rpm probe-results on page 237 show services rpm probe-results (BGP Neighbor Discovery) on page 238
Output Fields	Table 19 on page 234 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-<i>n</i> , where <i>n</i> is a cumulative number.
Target address	Destination address used for the probes.
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 .
Test size	Number of probes within a test.

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

Field Name	Field Description
Routing Instance Name	<p>(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured:</p> <ul style="list-style-type: none"> When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash (/) is used to separate the two entities. For example, if the routing instance called R1 is configured within the logical system called LS, the name in the output field is LS/R1. When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance. When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by default. A slash (/) is used to separate the two entities. For example, LS/default.
Probe results	<p>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:</p> <ul style="list-style-type: none"> Response received—Timestamp when the probe result was determined. Client and server hardware timestamps—If timestamps are configured, an entry appears at this point. Rtt—Average ping round-trip time (RTT), in microseconds. Egress jitter—Egress jitter, in microseconds. Ingress jitter—Ingress jitter, in microseconds. Round trip jitter—Round-trip jitter, in microseconds. Egress interarrival jitter—Egress interarrival jitter, in microseconds. Ingress interarrival jitter—Ingress interarrival jitter, in microseconds. Round trip interarrival jitter—Round-trip interarrival jitter, in microseconds.
Results over current test	<p>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.</p> <ul style="list-style-type: none"> Probes sent—Number of probes sent within the current test. Probes received—Number of probe responses received within the current test. Loss percentage—Percentage of lost probes for the current test. Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type icmp-ping-timestamp, the egress delay and ingress delay. <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> Samples—Number of probes. Minimum—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. Maximum—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. Average—Average RTT, ingress delay, or egress delay measured over the course of the current test. Peak to peak—Peak-to-peak difference, in microseconds. Stddev—Standard deviation, in microseconds. Sum—Statistical sum.

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

Field Name	Field Description
Results over last test	<p>Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed</p> <ul style="list-style-type: none"> • Probes sent—Number of probes sent for the most recently completed test. • Probes received—Number of probe responses received for the most recently completed test. • Loss percentage—Percentage of lost probes for the most recently completed test. • Test completed—Time the most recent test was completed. • Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type icmp-ping-timestamp, the egress delay and ingress delay. <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> • Samples—Number of probes. • Minimum—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test. • Maximum—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test. • Average—Average RTT, ingress delay, or egress delay measured for the most recently completed test. • Peak to peak—Peak-to-peak difference, in microseconds. • Stddev—Standard deviation, in microseconds. • Sum—Statistical sum.
Results over all tests	<p>Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.</p> <ul style="list-style-type: none"> • Probes sent—Number of probes sent in all tests. • Probes received—Number of probe responses received in all tests. • Loss percentage—Percentage of lost probes in all tests. • Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types icmp-ping-timestamp and udp-ping-timestamp, the egress delay and ingress delay. <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> • Samples—Number of probes. • Minimum—Minimum RTT, ingress delay, or egress delay measured over the course of the current test. • Maximum—Maximum RTT, ingress delay, or egress delay measured over the course of the current test. • Average—Average RTT, ingress delay, or egress delay measured over the course of the current test. • Peak to peak—Peak-to-peak difference, in microseconds. • Stddev—Standard deviation, in microseconds. • Sum—Statistical sum.

Sample Output

```

show services rpm probe-results user@host> show services rpm probe-results
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
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over last test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Test completed on Tue Feb  6 14:53:16 2007
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,

```

```

    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
Measurement: Positive Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Results over all tests:
Probes sent: 560, Probes received: 560, Loss percentage: 0
Measurement: Round trip time
    Samples: 560, Minimum: 805 usec, Maximum: 3114 usec, Average: 1756 usec,

    Peak to peak: 2309 usec, Stddev: 519 usec, Sum: xxxx usec
Measurement: Positive round trip jitter
    Samples: 257, Minimum: 0 usec, Maximum: 2054 usec, Average: 597 usec,
    Peak to peak: 2054 usec, Stddev: 427 usec, Sum: xxxx usec
Measurement: Negative round trip jitter
    Samples: 302, Minimum: 1 usec, Maximum: 1812 usec, Average: 511 usec,
    Peak to peak: 1811 usec, Stddev: 408 usec, Sum: xxxx usec
Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
Measurement: Positive Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
Measurement: Positive Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec

```

**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

CHAPTER 5

Ethernet OAM Link Fault Management

- [Ethernet OAM Link Fault Management—Overview on page 241](#)
- [Example of Ethernet OAM Link Fault Management Configuration on page 242](#)
- [Configuring Ethernet OAM Link Fault Management on page 245](#)
- [Configuration Statements for Ethernet OAM Link Fault Management on page 248](#)
- [Operational Commands for Ethernet OAM Link Fault Management on page 272](#)

Ethernet OAM Link Fault Management—Overview

- [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)

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.
- 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 246](#)
- [Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243](#)

Example of Ethernet OAM Link Fault Management Configuration

- [Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243](#)

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 243](#)
- [Overview and Topology on page 243](#)
- [Configuring Ethernet OAM Link Fault Management on Switch 1 on page 243](#)
- [Configuring Ethernet OAM Link Fault Management on Switch 2 on page 244](#)
- [Verification on page 245](#)

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.

Configuring Ethernet OAM Link Fault Management on Switch 1

CLI Quick Configuration

To quickly configure Ethernet OAM LFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management]
set interface ge-0/0/0
set interface ge-0/0/0 link-discovery active
set interface ge-0/0/0 pdu-interval 800
set interface ge-0/0/0 remote-loopback
```

Step-by-Step Procedure

To configure Ethernet OAM LFM on switch 1:

1. Enable IEEE 802.3ah OAM support on an interface:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0
```

2. Specify that the interface initiates the discovery process by configuring the link discovery mode to **active**:

```
[edit protocols oam ethernet link-fault-management]  
user@switch1# set interface ge-0/0/0 link-discovery active
```
3. Set the periodic OAM PDU-sending interval (in milliseconds) to 800 on switch 1:

```
[edit protocols oam ethernet link-fault-management]  
user@switch1# set interface pdu-interval 800
```
4. Set a remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes made to the frames. Ensure that the remote DTE supports remote loopback mode. To set the remote DTE in loopback mode

```
[edit protocols oam ethernet link-fault-management]  
user@switch1# set interface ge-0/0/0.0 remote-loopback
```

Results Check the results of the configuration:

```
[edit]  
user@switch1# show  
  
protocols {  
  oam {  
    ethernet {  
      link-fault-management {  
        interface ge-0/0/0 {  
          pdu-interval 800;  
          link-discovery active;  
          remote-loopback;  
        }  
      }  
    }  
  }  
}
```

Configuring Ethernet OAM Link Fault Management on Switch 2

CLI Quick Configuration To quickly configure Ethernet OAM LFM on switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management ]  
set interface ge-0/0/1  
set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Step-by-Step Procedure To configure Ethernet OAM LFM on switch 2:

1. Enable OAM on the peer interface on switch 2:

```
[edit protocols oam ethernet link-fault-management]  
user@switch2# set interface ge-0/0/1
```
2. Enable remote loopback support for the local interface:

```
[edit protocols oam ethernet link-fault-management]  
user@switch2# set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Results Check the results of the configuration:

```
[edit]
user@switch2# show

protocols {
  oam {
    ethernet {
      link-fault-management {
        interface ge-0/0/1 {
          negotiation-options {
            allow-remote-loopback;
          }
        }
      }
    }
  }
}
```

Verification

Verifying That OAM LFM Has Been Configured Properly

Purpose Verify that OAM LFM has been configured properly.

Action Use the `show oam ethernet link-fault-management` command:

```
user@switch1#show oam ethernet link-fault-management
```

Sample Output

```
Interface: ge-0/0/0.0
Status: Running, Discovery state: Send Any
Peer address: 00:19:e2:50:3b:e1
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote entity information:
Remote MUX action: forwarding, Remote parser action: forwarding
Discovery mode: active, Unidirectional mode: unsupported
Remote loopback mode: supported, Link events: supported
Variable requests: unsupported
```

Meaning When the output displays the MAC address and the discover state is **Send Any**, it means that OAM LFM has been configured properly.

- Related Documentation**
- [Configuring Ethernet OAM Link Fault Management \(CLI Procedure\) on page 246](#)
 - [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)

Configuring Ethernet OAM Link Fault Management

- [Configuring Ethernet OAM Link Fault Management \(CLI Procedure\) on page 246](#)

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: 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 interface-name 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
```

- 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 243](#)
 - [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)

Configuration Statements for Ethernet OAM Link Fault Management

- [\[edit protocols\] Configuration Statement Hierarchy on page 248](#)

[\[edit protocols\] Configuration Statement Hierarchy](#)

```
protocols {
  connections {
    remote-interface-switch connection-name {
      interface interface-name.unit-number;
      transmit-lsp label-switched-path;
      receive-lsp label-switched-path;
      no-autonegotiation;
    }
  }
  dcbx {
    disable;
    interface (all | interface-name) {
      disable;
      priority-flow-control {
        no-auto-negotiation;
      }
    }
  }
  dot1x {
    authenticator {
      authentication-profile-name profile-name;
      interface (all | [ interface-names ]) {
        disable;
        guest-vlan ( vlan-id | vlan-name );
        mac-radius <restrict>;
        maximum-requests number;
        no-reauthentication;
        quiet-period seconds;
        reauthentication {
          interval seconds;
        }
        retries number;
        server-fail (deny | permit | use-cache | vlan-id | vlan-name);
        server-reject-vlan ( vlan-id | vlan-name ) {
          eapol-block;
          block-interval block-interval;
        }
        server-timeout seconds;
        supplicant (multiple | single | single-secure);
        supplicant-timeout seconds;
        transmit-period seconds;
      }
    }
  }
}
```



```

no-mac-table-binding {
  authentication-profile-name
  interface
}
static mac-address {
  interface interface-name;
  vlan-assignment (vlan-id | vlan-name);
}
igmp-snooping {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
    flag flag (detail | disable | receive | send);
  }
  vlan (vlan-id | vlan-number) {
    data-forwarding {
      source {
        groups group-prefix;
      }
      receiver {
        source-vlans vlan-list;
        install;
      }
    }
  }
  disable {
    interface interface-name
  }
  immediate-leave;
  interface interface-name {
    group-limit limit;
    multicast-router-interface;
    static {
      group ip-address;
    }
  }
  proxy;
  query-interval seconds;
  query-last-member-interval seconds;
  query-response-interval seconds;
  robust-count number;
}
}
lldp {
  disable (LLDP);
  advertisement-interval seconds;
  hold-multiplier number;
  interface (LLDP) (all | interface-name) {
    disable (LLDP);
  }
  lldp-configuration-notification-interval seconds;
  management-address ip-management-address;
  ptopo-configuration-maximum-hold-time seconds;
  ptopo-configuration-trap-interval seconds;
  traceoptions (LLDP) {
    file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
  }
}

```

```
    flag flag (detail | disable | receive | send);
  }
}
lldp-med {
  disable;
  fast-start number;
  interface (all | interface-name) {
    disable;
    location {
      elin number;
      civic-based {
        what number;
        country-code code;
        ca-type {
          number {
            ca-value value;
          }
        }
      }
    }
  }
}
mpls {
  interface ( all | interface-name );
  label-switched-path lsp-name to remote-provider-edge-switch;
  path destination {
    <address | hostname> <strict | loose>
  }
}
mstp {
  disable;
  bpdu-block-on-edge;
  bridge-priority priority;
  configuration-name name;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    arp-on-stp
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  max-hops hops;
  msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
      disable;
      cost cost;
    }
  }
}
```

```

        edge;
        mode mode;
        priority priority;
    }
}
revision-level revision-level;
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}
}
mvrp {
    add-attribute-length-in-pdu
    disable
    interface (all | interface-name) {
        disable;
        join-timer milliseconds;
        leave-timer milliseconds;
        leaveall-timer milliseconds;
        registration (forbidden | normal);
    }
    no-dynamic-vlan;
    traceoptions {
        file filename <files number > <size size > <no-stamp | world-readable |
        no-world-readable>;
        flag flag;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            action-profile profile-name {
                default-actions {
                    interface-down;
                }
            }
        }
        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;
                    interval (10m | 10s | 1m | 1s | 100ms);
                    loss-threshold number;
                }
            }
            mep mep-id {
                auto-discovery;
                direction down;
                interface interface-name;
                remote-mep mep-id {

```

```
        action-profile profile-name;
      }
    }
  }
}
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;
    event-thresholds threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
  }
  negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
  }
}
}
}
rstp {
  disable;
  bpdu-block-on-edge;
  bridge-priority priority;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    disable;
    arp-on-stp
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    edge;
    mode mode;
    no-root-port;
```

```

        priority priority;
    }
    max-age seconds;
}
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}
}
sflow {
    agent-id;
    collector {
        ip-address;
        udp-port port-number;
    }
    disable;
    interfaces interface-name {
        disable;
        polling-interval seconds;
        sample-rate {
            egress number;
            ingress number;
        }
    }
    polling-interval seconds;
    sample-rate {
        egress number;
        ingress number;
    }
    source-ip;
}
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        arp-on-stp
            bpdu-timeout-action {
                block;
                log;
            }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
}
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}

```

```
}
uplink-failure-detection {
  group {
    group-name {
      link-to-monitor {
        interface-name;
      }
      link-to-disable {
        interface-name;
      }
    }
  }
}
vstp {
  bpdu-block-on-edge;
  disable;
  force-version stp;
  vlan (all | vlan-id | vlan-name) {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      arp-on-stp
        bpdu-timeout-action {
          log;
          block;
        }
      cost cost;
      disable;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    traceoptions {
      file filename <files number > <size size > <no-stamp | world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}
```

**Related
Documentation**

- [802.1X for EX Series Switches Overview](#)
- [Understanding Authentication on EX Series Switches](#)
- [Understanding Server Fail Fallback and Authentication on EX Series Switches](#)
- [IGMP Snooping on EX Series Switches Overview](#)
- [Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches](#)
- [Understanding MSTP for EX Series Switches](#)
- [Understanding Multiple VLAN Registration Protocol \(MVRP\) on EX Series Switches](#)

- [Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 279](#)
- [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)
- Understanding RSTP for EX Series Switches
- Understanding STP for EX Series Switches
- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)
- Understanding VSTP for EX Series Switches
- [Understanding Uplink Failure Detection on page 329](#)
- Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches

action

Syntax	<pre> action { syslog; link-down; } </pre>
Hierarchy Level	[edit protocols oam ethernet link-fault-management]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches.
Description	<p>Define the action or actions to be taken when the OAM link fault management (LFM) fault event occurs.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

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 246](#)

allow-remote-loopback

Syntax	allow-remote-loopback;
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<ul style="list-style-type: none">• Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

ethernet

```
Syntax ethernet {
    connectivity-fault-management {
        action-profile profile-name {
            default-actions {
                interface-down;
            }
        }
        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;
                    interval (10m | 10s | 1m | 1s | 100ms);
                    loss-threshold number;
                }
                mep mep-id {
                    auto-discovery;
                    direction down;
                    interface interface-name;
                    remote-mep mep-id {
                        action-profile profile-name;
                    }
                }
            }
        }
    }
    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;
            event-thresholds threshold-value;
            remote-loopback;
            event-thresholds {
```

```

        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
}
negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
}
}
}

```

Hierarchy Level [edit protocols [oam](#)]

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 243](#)
- [Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 281](#)
- [Configuring Ethernet OAM Link Fault Management \(CLI Procedure\) on page 246](#)
- [Configuring Ethernet OAM Connectivity Fault Management \(CLI Procedure\) on page 284](#)

event

Syntax	<pre>event { link-adjacency-loss; link-event-rate { frame-error <i>count</i>; frame-period <i>count</i>; frame-period-summary <i>count</i>; symbol-period <i>count</i>; } }</pre>
Hierarchy Level	[edit protocols oam ethernet link-fault-management action-profile <i>profile-name</i>]
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	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

event-thresholds

Syntax	<pre>event-thresholds { frame-error <i>count</i>; frame-period <i>count</i>; frame-period-summary <i>count</i>; symbol-period <i>count</i>; }</pre>
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

frame-error

Syntax	<code>frame-error count;</code>
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	<i>count</i> —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	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

frame-period

Syntax	<code>frame-period count;</code>
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	<i>count</i> —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	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

frame-period-summary

Syntax	<code>frame-period-summary count;</code>
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	<p>Configure the threshold value for sending frame period summary error events or taking the action specified in the action profile.</p> <p>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.</p>
Options	<p><i>count</i>—Threshold count in seconds for frame period summary error events.</p> <p>Range: 1 through 100 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

interface

Syntax	<pre> interface <i>interface-name</i> { link-discovery (active passive); pdu-interval <i>interval</i>; event-thresholds <i>threshold-value</i>; remote-loopback; event-thresholds { frame-error <i>count</i>; frame-period <i>count</i>; frame-period-summary <i>count</i>; symbol-period <i>count</i>; } negotiation-options { allow-remote-loopback; no-allow-link-events; } } </pre>
Hierarchy Level	[edit protocols oam ethernet link-fault-management]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches.
Description	<p>Configure Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.</p> <p>The remaining statements are explained separately.</p>
Options	<i>interface-name</i> —Name of the interface to be enabled for IEEE 802.3ah OAM link fault management (LFM) support.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243 • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

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	<ul style="list-style-type: none">• Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

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	<p><i>active</i>—In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality.</p> <p><i>passive</i>—In passive mode, the peer initiates the discovery process.</p> <p>Once the discovery process is initiated, both sides participate in discovery.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

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	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

link-event-rate

Syntax	<pre>link-event-rate { frame-error count; frame-period count; frame-period-summary count; symbol-period count; }</pre>
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	<p>Configure the number of link fault management (LFM) events per second.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

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;  
            event-thresholds threshold-value;  
            remote-loopback;  
            event-thresholds {  
                frame-error count;  
                frame-period count;  
                frame-period-summary count;  
                symbol-period count;  
            }  
        }  
        negotiation-options {  
            allow-remote-loopback;  
            no-allow-link-events;  
        }  
    }
```

Hierarchy Level [edit protocols [oam](#) [ethernet](#)]

Release Information Statement introduced in Junos OS Release 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 243](#)
- [Configuring Ethernet OAM Link Fault Management \(CLI Procedure\) on page 246](#)

negotiation-options

Syntax	negotiation-options { allow-remote-loopback; no-allow-link-events; }
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

no-allow-link-events

Syntax	no-allow-link-events;
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i> 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	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

oam

```

Syntax  oam {
    ethernet {
        connectivity-fault-management {
            action-profile profile-name {
                default-actions {
                    interface-down;
                }
            }
            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;
                        interval (10m | 10s | 1m | 1s | 100ms);
                        loss-threshold number;
                    }
                    mep mep-id {
                        auto-discovery;
                        direction down;
                        interface interface-name;
                        remote-mep mep-id {
                            action-profile profile-name;
                        }
                    }
                }
            }
        }
    }
    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;
            event-thresholds threshold-value;
            remote-loopback;
        }
    }
}

```

```

    event-thresholds {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
}
negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
}
}
}

```

Hierarchy Level	[edit protocols]
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	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243 • Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 281 • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246 • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284

pdu-interval

Syntax	<code>pdu-interval <i>interval</i>;</code>
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<i>interval</i> —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	<ul style="list-style-type: none">• Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

pdu-threshold

Syntax	<code>pdu-threshold <i>threshold-value</i>;</code>
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<i>threshold-value</i> —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	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

remote-loopback

Syntax	remote-loopback;
Hierarchy Level	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]
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	<ul style="list-style-type: none"> • Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243 • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

symbol-period

Syntax	symbol-period <i>count</i> ;
Hierarchy Level	[edit protocols oam ethernet link-fault-management action-profile <i>profile-name</i> ; event link-event-rate] , [edit protocols oam ethernet link-fault-management interface <i>interface-name</i> event-thresholds]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches.
Description	<p>Configure the threshold for sending symbol period events or taking the action specified in the action profile.</p> <p>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.</p>
Options	<p><i>count</i>—Threshold count in seconds for symbol period events.</p> <p>Range: 1 through 100 seconds</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

syslog

Syntax	syslog;
Hierarchy Level	[edit protocols oam ethernet link-fault-management action-profile <i>profile-name</i> ; 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	<ul style="list-style-type: none">• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246

Operational Commands for Ethernet OAM Link Fault Management

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	<ul style="list-style-type: none"> • Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 243 • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 246
List of Sample Output	show oam ethernet link-fault-management brief on page 277 show oam ethernet link-fault-management detail on page 277
Output Fields	Table 20 on page 273 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 20: show oam ethernet link-fault-management Output Fields

Field Name	Field Description	Level of Output
Status	Indicates the status of the established link. <ul style="list-style-type: none"> • Fail—A link fault condition exists. • Running—A link fault condition does not exist. 	All levels
Discovery state	State of the discovery mechanism: <ul style="list-style-type: none"> • Passive Wait • Send Any • Send Local Remote • Send Local Remote Ok 	All levels
Peer address	Address of the OAM peer.	All levels

Table 20: show oam ethernet link-fault-management Output Fields (*continued*)

Field Name	Field Description	Level of Output
Flags	Information about the interface. <ul style="list-style-type: none"> Remote-Stable—Indicates remote OAM client acknowledgment of, and satisfaction with local OAM state information. False indicates that remote DTE has either not seen or is unsatisfied with local state information. True indicates that remote DTE has seen and is satisfied with local state information. Local-Stable—Indicates local OAM client acknowledgment of, and satisfaction with remote OAM state information. False indicates that local DTE either has not seen or is unsatisfied with remote state information. True indicates that local DTE has seen and is satisfied with remote state information. Remote-State-Valid—Indicates the OAM client has received remote state information found within Local Information TLVs of received Information OAM PDUs. False indicates that OAM client has not seen remote state information. True indicates that the OAM client has seen remote state information. 	All levels
Remote loopback status	Indicates the remote loopback status. An OAM entity can put its remote peer into loopback mode using the Loopback control OAM PDU. In loopback mode, every frame received is transmitted back on the same port (except for OAM PDUs, which are needed to maintain the OAM session).	All levels
Remote entity information	Remote entity information. <ul style="list-style-type: none"> Remote MUX action—Indicates the state of the multiplexer functions of the OAM sublayer. Device is forwarding non-OAM PDUs to the lower sublayer or discarding non-OAM PDUs. Remote parser action—Indicates the state of the parser function of the OAM sublayer. Device is forwarding non-OAM PDUs to higher sublayer, looping back non-OAM PDUs to the lower sublayer, or discarding non-OAM PDUs. Discovery mode—Indicates whether discovery mode is active or inactive. Unidirectional mode—Indicates the ability to operate a link in a unidirectional mode for diagnostic purposes. Remote loopback mode—Indicates whether remote loopback is supported or not supported. Link events—Indicates whether interpreting link events is supported or not supported on the remote peer. Variable requests—Indicates whether variable requests are supported or not supported. The Variable Request OAM PDU, is used to request one or more MIB variables from the remote peer. 	All levels
OAM Receive Statistics		
Information	The number of information PDUs received.	detail
Event	The number of loopback control PDUs received.	detail
Variable request	The number of variable request PDUs received.	detail
Variable response	The number of variable response PDUs received.	detail
Loopback control	The number of loopback control PDUs received.	detail

Table 20: 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. The protocol default value is the number of symbols that can be received in one second on the underlying physical layer.	detail
Threshold	The number of errored symbols in the period required for the event to be generated.	detail
Errors in period	The number of symbol errors in the period reported in the received event PDU.	detail
Total errors	The number of errored symbols that have been reported in received event TLVs after the OAM sublayer was reset. Symbol errors are coding symbol errors.	detail
OAM Received Frame Error Event Information		
Events	The number of errored frame event TLVs that have been received after the OAM sublayer was reset.	detail
Window	The duration of the window in terms of the number of 100 ms period intervals.	detail
Threshold	The number of detected errored frames required for the event to be generated.	detail
Errors in period	The number of detected errored frames in the period.	detail

Table 20: show oam ethernet link-fault-management Output Fields (*continued*)

Field Name	Field Description	Level of Output
Total errors	The number of errored frames that have been reported in received event TLVs after the OAM sublayer was reset. A frame error is any frame error on the underlying physical layer.	detail
OAM Received Frame Period Error Event Information		
Events	The number of frame seconds errors event TLVs that have been received after the OAM sublayer was reset.	detail
Window	The duration of the frame seconds window.	detail
Threshold	The number of frame seconds errors in the period.	detail
Errors in period	The number of frame seconds errors in the period.	detail
Total errors	The number of frame seconds errors that have been reported in received event TLVs after the OAM sublayer was reset.	detail
OAM Transmitted Symbol Error Event Information		
Events	The number of symbol error event TLVs that have been transmitted after the OAM sublayer was reset.	detail
Window	The symbol error event window in the transmitted PDU.	detail
Threshold	The number of errored symbols in the period required for the event to be generated.	detail
Errors in period	The number of symbol errors in the period reported in the transmitted event PDU.	detail
Total errors	The number of errored symbols reported in event TLVs that have been transmitted after the OAM sublayer was reset.	detail
OAM Transmitted Frame Error Event Information		
Events	The number of errored frame event TLVs that have been transmitted after the OAM sublayer was reset.	detail
Window	The duration of the window in terms of the number of 100 ms period intervals.	detail
Threshold	The number of detected errored frames required for the event to be generated.	detail
Errors in period	The number of detected errored frames in the period.	detail
Total errors	The number of errored frames that have been detected after the OAM sublayer was reset.	detail

Sample Output

```

show oam ethernet link-fault-management brief
user@host> show oam ethernet link-fault-management brief
Interface: ge-0/0/1
Status: Running, Discovery state: Send Any
Peer address: 00:90:69:72:2c:83
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote loopback status: Disabled on local port, Enabled on peer port
Remote entity information:
  Remote MUX action: discarding, Remote parser action: loopback
  Discovery mode: active, Unidirectional mode: unsupported
  Remote loopback mode: supported, Link events: supported
  Variable requests: unsupported

show oam ethernet link-fault-management detail
user@host> show oam ethernet link-fault-management detail
Interface: ge-0/0/1
Status: Running, Discovery state: Send Any
Peer address: 00:90:69:0a:07:14
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
OAM receive statistics:
  Information: 186365, Event: 0, Variable request: 0, Variable response: 0
  Loopback control: 0, Organization specific: 0
OAM transmit statistics:
  Information: 186347, Event: 0, Variable request: 0, Variable response: 0
  Loopback control: 0, Organization specific: 0
OAM received symbol error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM received frame error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM received frame period error event information:
  Events: 0, Window: 0, Threshold: 0
  Errors in period: 0, Total errors: 0
OAM transmitted symbol error event information:
  Events: 0, Window: 0, Threshold: 1
  Errors in period: 0, Total errors: 0
OAM transmitted frame error event information:
  Events: 0, Window: 0, Threshold: 1
  Errors in period: 0, Total errors: 0
Remote entity information:
  Remote MUX action: forwarding, Remote parser action: forwarding
  Discovery mode: active, Unidirectional mode: unsupported
  Remote loopback mode: supported, Link events: supported
  Variable requests: unsupported

```


CHAPTER 6

Ethernet OAM Connectivity Fault Management

- [Ethernet OAM Connectivity Fault Management—Overview on page 279](#)
- [Example of Ethernet OAM Connectivity Fault Management Configuration on page 280](#)
- [Configuring Ethernet OAM Connectivity Fault Management on page 284](#)
- [Configuration Statements for Ethernet OAM Connectivity Fault Management on page 288](#)
- [Operational Commands for Ethernet OAM Connectivity Fault Management on page 308](#)

Ethernet OAM Connectivity Fault Management—Overview

- [Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 279](#)

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.

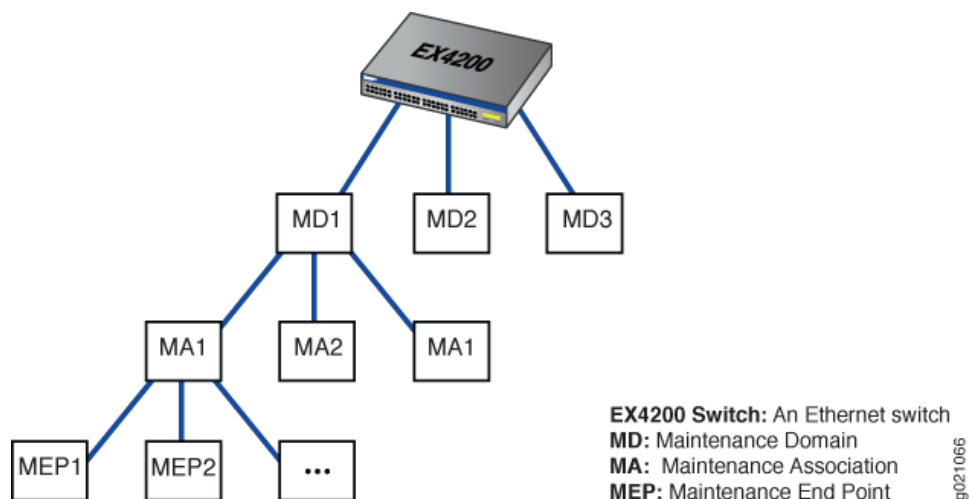
CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains. Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus 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 7 on page 280](#) shows the relationships among maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs) configured on a switch.

Figure 7: Relationship Among MEPs, MIPs, and Maintenance Domain Levels



Related Documentation

- [Configuring Ethernet OAM Connectivity Fault Management \(CLI Procedure\) on page 284](#)
- [Junos OS Network Interfaces Configuration Guide](#)

Example of Ethernet OAM Connectivity Fault Management Configuration

- [Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 281](#)

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

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 example describes how to enable and configure OAM CFM on a Gigabit Ethernet interface:

- [Requirements on page 281](#)
- [Overview and Topology on page 281](#)
- [Configuring Ethernet OAM Connectivity Fault Management on Switch 1 on page 281](#)
- [Configuring Ethernet OAM Connectivity Fault Management on Switch 2 on page 282](#)
- [Verification on page 283](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 10.2 or later for EX Series switches
- Two EX Series switches connected by a point-to-point Gigabit Ethernet link

Overview and Topology

CFM can be used to monitor the physical link between two switches. In the following example, two switches are connected by a point-to-point Gigabit Ethernet link. The link between these two switches is monitored using CFM.

Configuring Ethernet OAM Connectivity Fault Management on Switch 1

CLI Quick Configuration	To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:
	<pre>[edit protocols oam ethernet connectivity-fault-management maintenance-domain]set name-format character-string set maintenance-domain private level 0set maintenance-association private-maset continuity-check hold-interval 1s</pre>
Step-by-Step Procedure	To enable and configure OAM CFM on switch 1:
	<ol style="list-style-type: none"> Specify the maintenance domain name format: <pre>[edit protocols oam ethernet connectivity-fault-management maintenance-domain]user@switch1# set name-format character-string</pre>
	<ol style="list-style-type: none"> Specify the maintenance domain name and the maintenance domain level: <pre>[edit protocols oam ethernet connectivity-fault-management]user@switch1# set maintenance-domain private level 0</pre>
	<ol style="list-style-type: none"> Create a maintenance association: <pre>[edit protocols oam ethernet connectivity-fault-management maintenance-domain private]user@switch1# set maintenance-association private-ma</pre>

4. Enable the continuity check protocol and specify the continuity check hold interval:

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain private maintenance-association private-ma]user@switch1#
set continuity-check hold-interval 1s
```

5. Configure the maintenance association end point (MEP):

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain private maintenance-association private-ma]
user@switch1# set mep 100 interface ge-1/0/1 auto-discovery direction down
```

Results Check the results of the configuration.

```
[edit]
user@switch1# show

protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain private {
          level 0;
          maintenance-association private-ma {
            continuity-check {
              interval 1s;
            }
            mep 100 {
              interface ge-1/0/1;
              auto-discovery;
              direction down;
            }
          }
        }
      }
    }
  }
}
```

Configuring Ethernet OAM Connectivity Fault Management on Switch 2

CLI Quick Configuration To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]set
name-format character-string set maintenance-domain private level 0set
maintenance-association private-maset 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 100 interface ge-0/2/5 auto-discovery direction down
```

Results Check the results of the configuration.

```
[edit]
user@switch2# show

protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain private {
          level 0;
          maintenance-association private-ma {
            continuity-check {
              interval 1s;
            }
            mep 100 {
              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 283](#)

Verifying That OAM CFM Has Been Configured Properly

Purpose Verify that OAM CFM has been configured properly.

Action Use the show oam ethernet connectivity-fault-management interfaces detail command:

```
user@switch1# show oam ethernet connectivity-fault-management interfaces detail
```

Sample Output

```
Interface name: ge-1/0/1.0, Interface status: Active, Link status: Up
Maintenance domain name: private, Format: string, Level: 0
Maintenance association name: private-ma, Format: string
```

```
Continuity-check status: enabled, Interval: 1ms, Loss-threshold: 3 frames
MEP identifier: 100, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM                : no
  Erroneous CCM received                      : yes
  Cross-connect CCM received                  : no
  RDI sent by some MEP                        : yes
Statistics:
  CCMs sent                                  : 76
  CCMs received out of sequence               : 0
  LBMs sent                                  : 0
  Valid in-order LBRs received                : 0
  Valid out-of-order LBRs received            : 0
  LBRs received with corrupted data           : 0
  LBRs sent                                  : 0
  LTMs sent                                  : 0
  LTMs received                              : 0
  LTRs sent                                  : 0
  LTRs received                              : 0
  Sequence number of next LTM request         : 0
Remote MEP count: 2
Identifier  MAC address      State  Interface
2001       00:90:69:0b:7f:71  ok    ge-0/2/5.0
```

Meaning When the output displays 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 279](#)
- [Junos OS Network Interfaces Configuration Guide](#)

Configuring Ethernet OAM Connectivity Fault Management

- [Configuring Ethernet OAM Connectivity Fault Management \(CLI Procedure\) on page 284](#)

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 285](#)
2. [Configuring the Maintenance Domain MIP Half Function on page 285](#)
3. [Creating a Maintenance Association on page 286](#)
4. [Configuring the Continuity Check Protocol on page 286](#)
5. [Configuring a Maintenance Association End Point on page 286](#)

6. [Configuring a Connectivity Fault Management Action Profile on page 287](#)
7. [Configuring the Linktrace Protocol on page 288](#)

Creating the Maintenance Domain

A maintenance domain comprises network entities such as operators, providers, and customers. To enable connectivity fault management (CFM) on an Ethernet interface, you must create a maintenance domains, maintenance associations, and MEPs.

To create a maintenance domain:

1. Specify a name for the maintenance domain:

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

2. Specify a format for the maintenance domain name. If you specify **none**, no name is configured:

- A plain ASCII character string
- A domain name service (DNS) format
- A media access control (MAC) address plus a two-octet identifier in the range 0 through 65,535
- **none**

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

For example, to specify the name format as MAC address plus a two-octet identifier:

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name]
user@switch# set name-format mac+2oct
```

3. Configure the maintenance domain level, which is used to indicate the nesting relationship between this domain and other domains. Use a value from 0 through 7:

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

Configuring the Maintenance Domain MIP Half Function

MIP Half Function (MHF) divides the maintenance association intermediate point (MIP) functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loop-back and link-trace messages to help isolate faults. Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be the same.

To configure the MIP half function:

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

Creating a Maintenance Association

In a CFM maintenance domain, each service instance is called a maintenance association.

To create a maintenance association:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]
user@switch# set maintenance-association ma-name
```

Configuring the Continuity Check Protocol

The continuity check protocol is used for fault detection by a maintenance association end point (MEP) within a maintenance association. The MEP periodically sends continuity check multicast messages. The receiving MEPs use the continuity check messages (CCMs) to build a MEP database of all MEPs in the maintenance association.

To configure the continuity check protocol:

1. Enable the continuity check protocol:

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name]
user@switch# set continuity-check
```

2. Specify the continuity check hold interval. The hold interval is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name
continuity-check]
user@switch# set hold-interval number
```

3. Specify the CCM interval. The interval is the time between the transmission of CCMs. You can specify 10 minutes (10m), 1 minute (1m), 10 seconds (10s), 1 second (1s), 100 milliseconds (100ms), or 10 milliseconds (10ms).

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name
continuity-check]
user@switch# set interval number
```

4. Specify the number of CCMs (that is, protocol data units) that can be lost before the MEP is marked as down. The default number of protocol data units (PDUs) is 3.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name
continuity-check]
user@switch# set loss-threshold number
```

Configuring a Maintenance Association End Point

To configure a maintenance association end point:

1. Specify an ID for the MEP. The value can be from 1 through 8191.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name]
user@switch# set mep mep-id
```

2. Enable maintenance endpoint automatic discovery if you want to have the MEP accept continuity check messages (CCMs) from all remote MEPs of the same maintenance association:

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name mep mep-id]
user@switch# set auto-discovery
```

3. You can specify that CFM packets (CCMs) be transmitted only in one direction for the MEP, that is, the direction be set as **down** so that CCMs are transmitted only out of (not into) the interface configured on this MEP.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name mep mep-id]
user@switch# set direction down
```

4. Specify the logical interface to which the MEP is attached. It can be either an access interface or a trunk interface. If you specify a trunk interface, the VLAN associated with that interface must have a VLAN ID.



NOTE: You cannot associate an access interface that belongs to multiple VLANs with the MEP.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name mep mep-id]
user@switch# set interface interface-name
```

5. You can configure a remote MEP from which CCMs are expected. If autodiscovery is not enabled, the remote MEP must be configured under the **mep** statement. If the remote MEP is not configured under the **mep** statement, the CCMs from the remote MEP are treated as errors.

```
[edit protocols oam ethernet connectivity-fault-management
maintenance-domain domain-name maintenance-association ma-name mep mep-id]
user@switch# set remote-mep mep-id
```

Configuring a Connectivity Fault Management Action Profile

You can configure an action profile and specify the action to be taken when any of the configured events occur. Alternatively, you can configure an action profile and specify default actions when connectivity to a remote MEP fails.

To configure an action profile:

1. Specify a name for an action profile:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set action-profile profile-name
```

2. Configure the action of the action profile:

```
[edit protocols oam ethernet connectivity-fault-management action-profile
profile-name]
user@switch# set action interface-down
```

3. Configure one or more events under the action profile, the occurrence of which will trigger the corresponding action to be taken:

```
[edit protocols oam ethernet connectivity-fault-management action-profile
profile-name]
user@switch# set event event
```

See [Junos OS Network Interfaces Configuration Guide](#)

Configuring the Linktrace Protocol

The linktrace protocol is used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the **traceroute** command to verify the path between a pair of MEPs under the same maintenance association. Linktrace messages can also be used to verify the path between a MEP and a MIP under the same maintenance domain.

To configure the linktrace protocol:

1. Configure the linktrace path age timer. If no response to a linktrace request is received, the request and response entries are deleted after the age timer expires:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace age time
```

2. Configure the number of linktrace reply entries to be stored per linktrace request:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace path-database-size path-database-size
```

Related Documentation

- [Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 281](#)
- [Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 279](#)
- [Junos OS Network Interfaces Configuration Guide](#)

Configuration Statements for Ethernet OAM Connectivity Fault Management

- [\[edit protocols\] Configuration Statement Hierarchy on page 288](#)

[edit protocols] Configuration Statement Hierarchy

```
protocols {
  connections {
    remote-interface-switch connection-name {
      interface interface-name.unit-number;
      transmit-lsp label-switched-path;
      receive-lsp label-switched-path;
      no-autonegotiation;
```



```

    }
  }
  dcbx {
    disable;
    interface (all | interface-name) {
      disable;
      priority-flow-control {
        no-auto-negotiation;
      }
    }
  }
}
dot1x {
  authenticator {
    authentication-profile-name profile-name;
    interface (all | [ interface-names ]) {
      disable;
      guest-vlan ( vlan-id | vlan-name );
      mac-radius <restrict>;
      maximum-requests number;
      no-reauthentication;
      quiet-period seconds;
      reauthentication {
        interval seconds;
      }
      retries number;
      server-fail (deny | permit | use-cache | vlan-id | vlan-name);
      server-reject-vlan ( vlan-id | vlan-name ) {
        eapol-block;
        block-interval block-interval;
      }
      server-timeout seconds;
      supplicant (multiple | single | single-secure);
      supplicant-timeout seconds;
      transmit-period seconds;
    }
    no-mac-table-binding {
      authentication-profile-name
      interface
    }
    static mac-address {
      interface interface-name;
      vlan-assignment ( vlan-id | vlan-name );
    }
  }
  igmp-snooping {
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable>
        <match regex>;
      flag flag (detail | disable | receive | send);
    }
  }
  vlan ( vlan-id | vlan-number ) {
    data-forwarding {
      source {
        groups group-prefix;
      }
    }
    receiver {
      source-vlans vlan-list;
    }
  }
}

```

```
        install ;
    }
}
disable {
    interface interface-name
}
immediate-leave;
interface interface-name {
    group-limit limit;
    multicast-router-interface;
    static {
        group ip-address;
    }
}
proxy ;
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
}
}
lldp {
    disable (LLDP);
    advertisement-interval seconds;
    hold-multiplier number;
    interface (LLDP) (all | interface-name) {
        disable (LLDP);
    }
    lldp-configuration-notification-interval seconds;
    management-address ip-management-address;
    ptopo-configuration-maximum-hold-time seconds;
    ptopo-configuration-trap-interval seconds;
    traceoptions (LLDP) {
        file filename <files number> <size size> <world-readable | no-world-readable>
        <match regex>;
        flag flag (detail | disable | receive | send);
    }
}
lldp-med {
    disable;
    fast-start number;
    interface (all | interface-name) {
        disable;
        location {
            elin number;
            civic-based {
                what number;
                country-code code;
                ca-type {
                    number {
                        ca-value value;
                    }
                }
            }
        }
    }
}
}
```

```

}
mpls {
  interface ( all | interface-name );
  label-switched-path lsp-name to remote-provider-edge-switch;
  path destination {
    <address | hostname> <strict | loose>
  }
}
mstp {
  disable;
  bpdu-block-on-edge;
  bridge-priority priority;
  configuration-name name;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    arp-on-stp
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  max-hops hops;
  msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
      disable;
      cost cost;
      edge;
      mode mode;
      priority priority;
    }
  }
  revision-level revision-level;
  traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable |
      no-world-readable>;
    flag flag;
  }
}
mvrp {
  add-attribute-length-in-pdu
  disable
  interface (all | interface-name) {
    disable;
    join-timer milliseconds;
    leave-timer milliseconds;
    leaveall-timer milliseconds;
    registration (forbidden | normal);
  }
}

```

```

    }
    no-dynamic-vlan;
    traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable |
        no-world-readable>;
        flag flag;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            action-profile profile-name {
                default-actions {
                    interface-down;
                }
            }
        }
        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;
                    interval (10m | 10s | 1m | 1s | 100ms);
                    loss-threshold number;
                }
                mep mep-id {
                    auto-discovery;
                    direction down;
                    interface interface-name;
                    remote-mep mep-id {
                        action-profile profile-name;
                    }
                }
            }
        }
    }
}
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;
event-thresholds 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;
}
}
}
}
rstp {
    disable;
    bpdu-block-on-edge;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        arp-on-stp
            bpdu-timeout-action {
                block;
                log;
            }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
}
traceoptions {
    file filename <files number> <size size> <no-stamp | world-readable |
        no-world-readable>;
    flag flag;
}
}
sflow {
    agent-id;
    collector {
        ip-address;
        udp-port port-number;
    }
    disable;
    interfaces interface-name {
        disable;
        polling-interval seconds;
        sample-rate {
```

```
        egress number;  
        ingress number;  
    }  
}  
polling-interval seconds;  
sample-rate {  
    egress number;  
    ingress number;  
}  
source-ip;  
}  
stp {  
    disable;  
    bridge-priority priority;  
    forward-delay seconds;  
    hello-time seconds;  
    interface (all | interface-name) {  
        disable;  
        arp-on-stp  
            bpdv-timeout-action {  
                block;  
                log;  
            }  
        cost cost;  
        edge;  
        mode mode;  
        no-root-port;  
        priority priority;  
    }  
    max-age seconds;  
}  
traceoptions {  
    file filename <files number > <size size > <no-stamp | world-readable |  
        no-world-readable>;  
    flag flag;  
}  
uplink-failure-detection {  
    group {  
        group-name {  
            link-to-monitor {  
                interface-name;  
            }  
            link-to-disable {  
                interface-name;  
            }  
        }  
    }  
}  
vstp {  
    bpdv-block-on-edge;  
    disable;  
    force-version stp;  
    vlan (all | vlan-id | vlan-name) {  
        bridge-priority priority;  
        forward-delay seconds;  
        hello-time seconds;  
    }  
}
```

```

interface (all | interface-name) {
  arp-on-stp
    bpdtimeout-action {
      log;
      block;
    }
  cost cost;
  disable;
  edge;
  mode mode;
  no-root-port;
  priority priority;
}
max-age seconds;
traceoptions {
  file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
  flag flag;
}
}
}

```

Related Documentation

- 802.1X for EX Series Switches Overview
- Understanding Authentication on EX Series Switches
- Understanding Server Fail Fallback and Authentication on EX Series Switches
- IGMP Snooping on EX Series Switches Overview
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches
- Understanding MSTP for EX Series Switches
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches
- [Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 279](#)
- [Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 241](#)
- Understanding RSTP for EX Series Switches
- Understanding STP for EX Series Switches
- [Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 67](#)
- Understanding VSTP for EX Series Switches
- [Understanding Uplink Failure Detection on page 329](#)
- Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches

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

Syntax	<pre>action-profile <i>profile-name</i> { default-actions { interface-down; } }</pre>
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 a name and default action for an action profile.
Options	<p><i>profile-name</i>—Name of the action profile.</p> <p><i>default-actions</i>—Defines the action to be taken when connectivity to the remote MEP is lost.</p> <p><i>interface-down</i>—Brings the interface down when a remote MEP connectivity failure is detected.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

age (EX Series Switch Only)

Syntax	<pre>age (30m 10m 1m 30s 10s);</pre>
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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• 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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

connectivity-fault-management (EX Series Switch Only)

```
Syntax connectivity-fault-management {
    action-profile profile-name {
        default-actions {
            interface-down;
        }
    }
    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;
                interval (10m | 10s | 1m | 1s | 100ms);
                loss-threshold number;
            }
            mep mep-id {
                auto-discovery;
                direction down;
                interface interface-name;
                remote-mep mep-id {
                    action-profile profile-name;
                }
            }
        }
    }
}
```

Hierarchy Level [edit protocols [oam](#) [ethernet](#)]

Release Information Statement introduced in Junos OS Release 10.2 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 284](#)
- [Junos OS Network Interfaces Configuration Guide](#)

continuity-check (EX Series Switch Only)

Syntax	<pre>continuity-check { hold-interval <i>minutes</i>; interval (10m 10s 1m 1s 100ms); loss-threshold <i>number</i>; }</pre>
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	<p>Specify continuity check protocol options.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

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	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

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

Syntax	hold-interval <i>minutes</i> ;
Hierarchy Level	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>domain-name</i> maintenance-association <i>ma-name</i> 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	<i>minutes</i> —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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

interface (OAM CFM, for EX Series Switch Only)

Syntax	interface (<i>interface-name</i> ((ge- xe-) (<i>fpc/pic/port</i> <i>fpc/pic/port.unit-number</i> <i>fpc/pic/port.unit-number</i> vlan <i>vlan-id</i>)));
Hierarchy Level	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>domain-name</i> maintenance-association <i>ma-name</i> mep <i>mep-id</i>]
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	<i>interface-name</i> —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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

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	<p>10m—10 minutes.</p> <p>10s—10 seconds.</p> <p>1m—1 minute.</p> <p>1s—1 second.</p> <p>100ms—100 milliseconds.</p> <p>10ms—10 milliseconds.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

level (EX Series Switch Only)

Syntax	level <i>number</i> ;
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	<p>number—Number used to identify the maintenance domain to which the CFM message belongs.</p> <p>Range: 0 through 7</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

linktrace (EX Series Switch Only)

Syntax	linktrace { age (30m 10m 1m 30s 10s); path-database-size <i>path-database-size</i> ; }
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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

loss-threshold (EX Series Switch Only)

Syntax	loss-threshold <i>number</i> ;
Hierarchy Level	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>domain-name</i> maintenance-association <i>ma-name</i> 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	<i>number</i> —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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

maintenance-association (EX Series Switch Only)

Syntax	<pre> maintenance-association <i>ma-name</i> { continuity-check { hold-interval <i>minutes</i>; interval (10m 10s 1m 1s 100ms); loss-threshold <i>number</i>; } mep <i>mep-id</i> { auto-discovery; direction down; interface <i>interface-name</i>; remote-mep <i>mep-id</i> { action-profile <i>profile-name</i>; } } } </pre>
Hierarchy Level	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>domain-name</i>]
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	<p><i>ma-name</i>—The name of the maintenance association within the maintenance domain.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

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;
 interval (10m | 10s | 1m | 1s | 100ms);
 loss-threshold number;
 }
 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 284](#)
- [Junos OS Network Interfaces Configuration Guide](#)

mep (EX Series Switch Only)

Syntax	<pre> mep <i>mep-id</i> { auto-discovery; direction down; interface <i>interface-name</i>; remote-mep <i>mep-id</i> { action-profile <i>profile-name</i>; } } </pre>
Hierarchy Level	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>domain-name</i> maintenance-association <i>ma-name</i>]
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	<p>mep-id—Numeric identifier of the MEP.</p> <p>Range: 1 through 8191</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 Junos OS Network Interfaces Configuration Guide

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 <i>domain-name</i>]
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	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

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 <i>domain-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2 for EX Series switches.
Description	Specify the format of the maintenance domain name.
Options	<p>character-string—The name is an ASCII character string.</p> <p>none—Name format none means that maintenance domain name is not used.</p> <p>dns—Name is in domain name service (DNS) format. For example: www.juniper.net.</p> <p>mac+2oct—Name is the MAC address plus a two-octet maintenance association identifier. For example: 08:00:22:33:44:55.100.</p> <p>Default: character-string</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

path-database-size (EX Series Switch Only)

Syntax	path-database-size <i>path-database-size</i> ;
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	<p>path-database-size—Database size (number of entries stored per request).</p> <p>Range: 1 through 500</p> <p>Default: 100</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284 • Junos OS Network Interfaces Configuration Guide

remote-mep (EX Series Switch Only)

Syntax	<code>remote-mep mep-id { action-profile profile-name; }</code>
Hierarchy Level	[edit protocols <code>oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id</code>]
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	<p>mep-id—Specify the numeric identifier of the MEP.</p> <p>Range: 1 through 8191</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 284• Junos OS Network Interfaces Configuration Guide

Operational Commands for Ethernet OAM Connectivity Fault Management

clear oam ethernet connectivity-fault-management statistics

Syntax	clear oam ethernet connectivity-fault-management statistics <interface <i>ethernet-interface-name</i> > <level <i>md-level</i> >
Release Information	Command introduced in Junos OS Release 10.2 for EX Series switches.
Description	Clear all statistics maintained by CFM.
Options	<p>interface <i>ethernet-interface-name</i>—(Optional) Clear CFM statistics only for MEPs attached to the specified Ethernet physical interface.</p> <p>level <i>level</i>—(Optional) Clear CFM statistics only for MEPs within CFM maintenance domains (MDs) of the specified level.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show oam ethernet connectivity-fault-management interfaces on page 314 • show oam ethernet connectivity-fault-management linktrace path-database on page 320 • show oam ethernet connectivity-fault-management mip on page 328
List of Sample Output	clear oam ethernet connectivity-fault-management statistics on page 309
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
```

show oam ethernet connectivity-fault-management forwarding-state

Syntax	show oam ethernet connectivity-fault-management forwarding-state <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	<p>interface <i>interface-name</i>—Display forwarding state information for the specified Ethernet interface only.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear oam ethernet connectivity-fault-management statistics on page 309 • show oam ethernet connectivity-fault-management linktrace path-database on page 320 • show oam ethernet connectivity-fault-management mip on page 328
List of Sample Output	<p>show oam ethernet connectivity-fault-management forwarding-state on page 311</p> <p>show oam ethernet connectivity-fault-management forwarding-state interface on page 311</p> <p>show oam ethernet connectivity-fault-management forwarding-state interface detail on page 312</p> <p>show oam ethernet connectivity-fault-management forwarding-state interface interface-name on page 312</p>
Output Fields	Table 21 on page 310 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 21: 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

Table 21: 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 type   Nexthop index
0
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 type   Nexthop index
0
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 type   Nexthop index
0
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 type	Nexthop index
0		Drop	none	
1		Drop	none	
2		Drop	none	
3		Drop	none	

4		Drop	none
5		Drop	none
6		Drop	none
7	down	Receive	none

show oam ethernet connectivity-fault-management interfaces

Syntax	show oam ethernet connectivity-fault-management interfaces <ethernet-interface-name> <level md-level> <brief detail extensive>
Release Information	Command introduced in Junos OS Release 10.2 for EX Series switches.
Description	Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for Ethernet interfaces.
Options	<p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>ethernet-interface-name—(Optional) Display CFM information only for CFM entities attached to the specified Ethernet interface.</p> <p>level md-level—(Optional) Display CFM information for CFM identities enclosed within a maintenance domain of the specified level.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear oam ethernet connectivity-fault-management statistics on page 309 • show oam ethernet connectivity-fault-management linktrace path-database on page 320 • show oam ethernet connectivity-fault-management mip on page 328
List of Sample Output	show oam ethernet connectivity-fault-management interfaces on page 317 show oam ethernet connectivity-fault-management interfaces detail on page 318 show oam ethernet connectivity-fault-management interfaces extensive on page 318 show oam ethernet connectivity-fault-management interfaces level on page 319 show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces) on page 319
Output Fields	Table 22 on page 314 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 22: 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

Table 22: show oam ethernet connectivity-fault-management interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Maintenance domain name	Maintenance domain name.	detail extensive
Format (Maintenance domain)	Maintenance domain name format configured.	detail extensive
Level	Maintenance domain level configured.	All levels
Maintenance association name	Maintenance association name.	detail extensive
Format (Maintenance association)	Maintenance association name format configured.	detail extensive
Continuity-check status	Continuity-check status.	detail extensive
Interval	Continuity-check message interval.	detail extensive
Loss-threshold	Lost continuity-check message threshold.	detail extensive
MEP identifier	Maintenance association end point (MEP) identifier.	All levels
Neighbours	Number of MEP neighbors.	All levels
Direction	MEP direction configured.	detail extensive
MAC address	MAC address configured for the MEP.	detail extensive
MEP status	Indicates the status of the Connectivity Fault Management (CFM) protocol running on the MEP: Running , inactive , disabled , or unsupported .	detail extensive
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

Table 22: show oam ethernet connectivity-fault-management interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
CCMs received out of sequence	Number of CCMs received out of sequence.	detail extensive
LBM 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
LTM sent	Linktrace messages (LTMs) transmitted.	detail extensive
LTM received	Linktrace messages received.	detail extensive
LTR sent	Linktrace responses (LTRs) transmitted.	detail extensive
LTR 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	<p>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.</p> <p>For all other cases, this field displays 0.</p>	detail extensive
Valid 1DMs received	<p>If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of valid 1DM frames received.</p> <p>For all other cases, this field displays 0.</p>	detail extensive
Invalid 1DMs received	<p>If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of invalid 1DM frames received.</p> <p>For all other cases, this field displays 0.</p>	detail extensive
DMMs sent	<p>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.</p> <p>For all other cases, this field displays 0.</p>	detail extensive

Table 22: show oam ethernet connectivity-fault-management interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
DMRs sent	If the interface is attached to a responder MEP for a two-way ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays 0.	detail extensive
Valid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays 0.	detail extensive
Invalid DMRs received	If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays 0.	detail extensive
Remote MEP count	Number of remote MEPs.	extensive
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 Identifier	Neighbours
ge-1/1/0.0	Up	Active	0	2	1
ge-1/1/0.1	Up	Active	0	2	1
ge-1/1/0.10	Up	Active	0	2	1
ge-1/1/0.100	Up	Active	0	2	1
ge-1/1/0.101	Up	Active	0	2	1
ge-1/1/0.102	Up	Active	0	2	1
ge-1/1/0.103	Up	Active	0	2	1
ge-1/1/0.104	Up	Active	0	2	1
ge-1/1/0.105	Up	Active	0	2	1
ge-1/1/0.106	Up	Active	0	2	1
...					

```

show oam ethernet connectivity-fault-management interfaces detail
user@host> show oam ethernet connectivity-fault-management interfaces detail
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
Maintenance domain name: md0, Format: string, Level: 5
Maintenance association name: ma1, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM                : no
  Erroneous CCM received                      : yes
  Cross-connect CCM received                  : no
  RDI sent by some MEP                       : yes
Statistics:
  CCMs sent                                  : 76
  CCMs received out of sequence               : 0
  LBMs sent                                  : 0
  Valid in-order LBRs received                : 0
  Valid out-of-order LBRs received            : 0
  LBRs received with corrupted data           : 0
  LBRs sent                                   : 0
  LTMs sent                                  : 0
  LTMs received                              : 0
  LTRs sent                                  : 0
  LTRs received                              : 0
  Sequence number of next LTM request         : 0
  1DMs sent                                   : 0
  Valid 1DMs received                        : 0
  Invalid 1DMs received                      : 0
  DMMs sent                                  : 0
  DMRs sent                                  : 0
  Valid DMRs received                       : 0
  Invalid DMRs received                     : 0
Remote MEP count: 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      : 0
1DMs sent                               : 0
Valid 1DMs received                      : 0
Invalid 1DMs received                   : 0
DMMs sent                               : 0
DMRs sent                               : 0
Valid DMRs received                     : 0
Invalid DMRs received                   : 0
Remote MEP count: 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 7
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, vln 100    Up        Active      5          100      0
ge-10/3/10.4091, vln 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 vln 100
Interface      Link      Status      Level      MEP      Neighbours
Identifier
ge-4/0/1.0, vln 100    Up        Active      5          100      0

```

```

user@host> show oam ethernet connectivity-fault-management interfaces ge-10/3/10.4091 vln 4091
Interface      Link      Status      Level      MEP      Neighbours
Identifier
ge-10/3/10.4091, vln 4091 Down      Inactive    4          400      0

```

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

Syntax	show oam ethernet connectivity-fault-management path-database <i>host</i> maintenance-association <i>ma-name</i> maintenance-domain <i>md-name</i> <i>mac-address</i>
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	<p><i>mac-address</i>—Display connectivity fault management path database information for the specified MAC address of the remote host.</p> <p><i>maintenance-association</i> <i>ma-name</i>—Display connectivity fault management path database information for the specified maintenance association.</p> <p><i>maintenance-domain</i> <i>md-name</i>—Display connectivity fault management path database information for the specified maintenance domain.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear oam ethernet connectivity-fault-management statistics on page 309 • show oam ethernet connectivity-fault-management interfaces on page 314 • show oam ethernet connectivity-fault-management mip on page 328
List of Sample Output	show oam ethernet connectivity-fault-management path-database on page 321 show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands) on page 321
Output Fields	Table 23 on page 320 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 23: 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.

Table 23: 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
tracertool
Commands)
user@host> show oam ethernet connectivity-fault-management path-database
maintenance-domain MD2 maintenance-association MA2 00:06:07:08:09:0A
Linktrace to 00:06:07:08:09:0A, Interface : ge-5/0/1.0
Maintenance Domain: MD2, Level: 6
Maintenance Association: MA2, Local Mep: 10

Hop      TTL      Source MAC address      Next hop MAC address
Transaction Identifier:100002
1        63      00:00:aa:aa:aa:aa      00:00:bb:bb:bb:bb
2        62      00:00:bb:bb:bb:bb      00:00:cc:cc:cc:cc
3        61      00:00:cc:cc:cc:cc      00:06:07:08:09:0A
4        60      00:06:07:08:09:0A      00:00:00:00:00:00
Transaction Identifier:100003
1        63      00:00:aa:aa:aa:aa      00:00:bb:bb:bb:bb
2        62      00:00:bb:bb:bb:bb      00:00:cc:cc:cc:cc
3        61      00:00:cc:cc:cc:cc      00:06:07:08:09:0A
4        60      00:06:07:08:09:0A      00:00:00:00:00:00

```

show oam ethernet connectivity-fault-management mep-database

Syntax	<pre>show oam ethernet connectivity-fault-management mep-database maintenance-domain <i>domain-name</i> maintenance-association <i>ma-name</i> <local-mep <i>local-mep-id</i>> <remote-mep <i>remote-mep-id</i>></pre>
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	<p><i>maintenance-association ma-name</i>—Display connectivity fault management information for the specified maintenance association.</p> <p><i>maintenance-domain domain-name</i>—Display connectivity fault management information for the specified maintenance domain.</p> <p><i>local-mep local-mep-id</i>—(Optional) Display connectivity fault management information for the specified local MEP only.</p> <p><i>remote-mep remote-mep-id</i>—(Optional) Display connectivity fault management information for the specified remote MEP only.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear oam ethernet connectivity-fault-management statistics on page 309 • show oam ethernet connectivity-fault-management interfaces on page 314 • show oam ethernet connectivity-fault-management mip on page 328
List of Sample Output	<p>show oam ethernet connectivity-fault-management mep-database on page 326</p> <p>show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 326</p> <p>show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event) on page 326</p>
Output Fields	Table 24 on page 322 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 24: show oam ethernet connectivity-fault-management mep-database Output Fields

Field Name	Field Description
Maintenance domain name	Maintenance domain name.

Table 24: 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.

Table 24: 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	<p>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.</p> <p>For all other cases, this field displays 0.</p>
Valid 1DMs received	<p>If the MEP is a receiver for a one-way ETH-DM session: Number of valid 1DM frames received.</p> <p>For all other cases, this field displays 0.</p>
Invalid 1DMs received	<p>If the MEP is a receiver for a one-way ETH-DM session: Number of invalid 1DM frames received.</p> <p>For all other cases, this field displays 0.</p>
DMMs sent	<p>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.</p> <p>For all other cases, this field displays 0.</p>
DMRs sent	<p>If the MEP is a responder for a ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent.</p> <p>For all other cases, this field displays 0.</p>

Table 24: 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. For all other cases, this field displays 0.
Invalid DMRs received	If the MEP is an initiator for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays 0.
Remote MEP identifier	MEP identifier of the remote MEP.
State (remote MEP)	State of the remote MEP: idle , start , ok , or failed .
MAC address	MAC address of the remote MEP.
Type	Whether the remote MEP MAC address was learned using automatic discovery or configured.
Interface	Interface of the remote MEP. A seven-digit number is appended if CFM is configured to run on a routing instance of type VPLS.
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	<ul style="list-style-type: none"> In the Maintenance domain section, displays the last transmitted port status TLV value. In the Remote MEP section, displays the last value of port status TLV received from the remote MEP. <p>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.</p>
Interface status TLV	<ul style="list-style-type: none"> In the Maintenance domain section, displays the last transmitted interface status TLV value. In the Remote MEP section, displays the last value of interface status TLV received from the remote MEP. <p>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.</p>
Action profile	Name of the action profile occurrence associated with a remote MEP.
Last event	When an action profile occurs, displays the last event that triggered it.
Last event cleared	When all the configured and occurred events (under action profile) are cleared, then the action taken gets reverted (such as down interface is made up) and the corresponding time is noted and displayed.
Action	Action taken and the corresponding time of the action occurrence.

Sample Output

```

show oam ethernet connectivity-fault-management mep-database
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
Maintenance association name: vpls-vlan200, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
Auto-discovery: enabled, Priority: 0
Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up
Defects:
  Remote MEP not receiving CCM                : no
  Erroneous CCM received                      : no
  Cross-connect CCM received                  : no
  RDI sent by some MEP                       : no
Statistics:
  CCMS sent                                  : 1476
  CCMS received out of sequence              : 0
  LBMS sent                                  : 85
  Remote MEP count: 1
  Identifier   MAC address   State   Interface
  100         00:19:e2:b2:81:4b   ok     vt-0/1/10.1049088

show oam ethernet connectivity-fault-management mep-database
local-mep remote-mep
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200 local-mep 200
remote-mep 100
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
Maintenance association name: vpls-vlan200, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
Auto-discovery: enabled, Priority: 0
Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up

Remote MEP identifier: 100, State: ok
MAC address: 00:19:e2:b2:81:4b, Type: Learned
Interface: vt-0/1/10.1049088
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: none

show oam ethernet connectivity-fault-management mep-database
remote-mep
(Action Profile Event)
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 remote-mep 200
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
Auto-discovery: enabled, Priority: 0
Interface status TLV: none, Port status TLV: none
Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

Remote MEP identifier: 200, State: ok
MAC address: 00:05:85:73:96:1f, Type: Configured
Interface: ge-1/0/8.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: lower-layer-down
Action profile: juniper

```

Last event: Interface-status-tlv lower-layer-down
Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)

show oam ethernet connectivity-fault-management mip

Syntax	show oam ethernet connectivity-fault-management mip <qualifier>
Release Information	Command introduced in Junos OS Release 10.2 for EX Series switches.
Description	Display all the maintenance association intermediate points (MIPs) created in the system. Specify qualifiers to display specific MIPs.
Options	<i>qualifier</i> —(Optional) Display the specified MIP.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show oam ethernet connectivity-fault-management interfaces on page 314 • show oam ethernet connectivity-fault-management linktrace path-database on page 320
List of Sample Output	show oam ethernet connectivity-fault-management mip on page 328
Output Fields	Table 25 on page 328 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 25: 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

```

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

```


CHAPTER 7

Uplink Failure Detection

- [Uplink Failure Detection—Overview on page 329](#)
- [Configuring Uplink Failure Detection on page 331](#)
- [Verifying Uplink Failure Detection on page 332](#)
- [Configuration Statements for Uplink Failure Detection on page 334](#)
- [Operational Commands for Uplink Failure Detection on page 335](#)

Uplink Failure Detection—Overview

- [Understanding Uplink Failure Detection on page 329](#)

Understanding Uplink Failure Detection

Uplink failure detection allows an EX Series switch to detect link failure on uplink interfaces and to propagate the failure to the downlink interfaces so that servers connected to those downlinks 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:

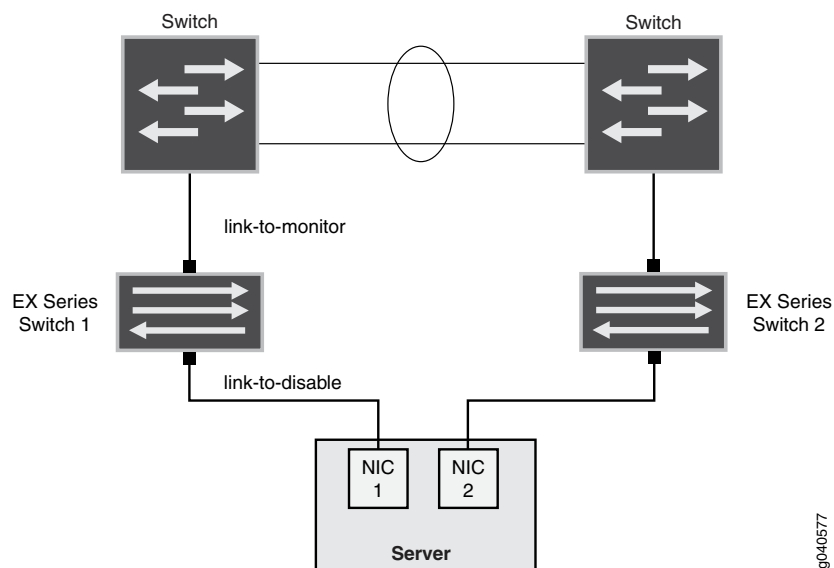
- [Uplink Failure Detection Overview on page 329](#)
- [Failure Detection Pair on page 330](#)

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 bound to the uplink interface. A server that is connected to the disabled downlink interface triggers a network-adapter failover to a secondary link to avoid any information drop.

[Figure 8 on page 330](#) illustrates a typical setup for uplink failure detection.

Figure 8: 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 into separate groups.



NOTE: For logical interfaces, the server must run some high level protocol such as keepalives between switch and server to detect failure of logical links.

Failure Detection Pair

Uplink failure detection requires that you create pairs of uplink and downlink interfaces in a group. Each pair includes one of each of the following:

- A link-to-monitor interface—The link-to-monitor interfaces specify the uplinks the switch monitors. You can configure a maximum of eight uplink interfaces as link-to-monitor for a group.

- A link-to-disable interface—The link-to-disable interfaces specify the downlinks the switch disables when the switch detects an uplink failure. You can configure a maximum of eight downlink interfaces as link-to-disable for 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 331](#)

Configuring Uplink Failure Detection

- [Configuring Interfaces for Uplink Failure Detection \(CLI Procedure\) on page 331](#)

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 downlinks can switch over to secondary interfaces.

Follow these configuration guidelines:

- Configure an interface in only one group.
- Configure a maximum of eight groups for each switch.
- Configure a maximum of eight uplinks and eight downlinks in each group.
- Configure physical links and logical links in separate groups.



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 an uplink-failure-detection 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 each uplink interface you add to the group.
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 3 for each downlink interface you add to the group.



NOTE: After you have configured an uplink-failure-detection group, use the `show uplink-failure-detection group group-name` command to verify that all interfaces in the group are up. If the interfaces are down, uplink failure detection does not work.

**Related
Documentation**

- [Verifying That Uplink Failure Detection Is Working Correctly on page 332](#)
- [Understanding Uplink Failure Detection on page 329](#)

Verifying Uplink Failure Detection

- [Verifying That Uplink Failure Detection Is Working Correctly on page 332](#)

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 331](#)
 - [Understanding Uplink Failure Detection on page 329](#)

Configuration Statements for Uplink Failure Detection

group

Syntax	<code>group <i>group-name</i> { link-to-monitor <i>interface-name</i>; link-to-disable <i>interface-name</i>; }</code>
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	<i>group-name</i> —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	<ul style="list-style-type: none">• Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 331

link-to-disable

Syntax	<code>link-to-disable <i>interface-name</i>;</code>
Hierarchy Level	[edit protocols uplink-failure-detection group <i>group-name</i>]
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 eight downlink interfaces in a group.
Options	<i>interface-name</i> —Name of the downlink interface in the uplink-failure-detection 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	<ul style="list-style-type: none">• Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 331

link-to-monitor

Syntax	<code>link-to-monitor <i>interface-name</i>;</code>
Hierarchy Level	<code>[edit protocols uplink-failure-detection group <i>group-name</i>]</code>
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 eight uplink interfaces in a group.
Options	<i>interface-name</i> —Name of the uplink interface in the uplink-failure-detection 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	<ul style="list-style-type: none"> • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 331

uplink-failure-detection

Syntax	<pre>uplink-failure-detection { group <i>group-name</i> { link-to-monitor <i>interface-name</i>; link-to-disable <i>interface-name</i>; } }</pre>
Hierarchy Level	<code>[edit protocols]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for EX Series switches.
Description	<p>Configure uplink and downlink interfaces in a group to monitor uplink failures and to propagate uplink failures to the downlink interfaces.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 331

Operational Commands for Uplink Failure Detection

show uplink-failure-detection

Syntax	<code>show uplink-failure-detection</code> <code><group group-name></code>
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	<ul style="list-style-type: none"> Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 331
List of Sample Output	show uplink-failure-detection on page 336
Output Fields	Table 26 on page 336 lists the output fields for the show uplink-failure-detection command. Output fields are listed in the approximate order in which they appear.

Table 26: show uplink-failure-detection Output Fields

Field Name	Field Description
Group	Name of the group.
Uplink	The uplink interface or interfaces configured as link-to-monitor. NOTE: The asterisk (*) indicates that the link is up.
Downlink	The downlink interface or interfaces configured as link-to-disable. NOTE: The asterisk (*) indicates that the link is up.
Failure Action	Status of uplink failure detection: <ul style="list-style-type: none"> Active—The switch has detected an uplink failure and has brought the downlink down. Inactive—The uplink or uplinks are up.

Sample Output

```

user@switch> show uplink-failure-detection
uplink-failure-detection Group      : group1
                        Uplink      : ge-0/0/0*
                        Downlink    : ge-0/0/1*
                        Failure Action : Inactive

                        Group      : group2

```


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

Monitoring General Network Traffic and Hosts

- [Monitoring Hosts Using the J-Web Ping Host Tool on page 339](#)
- [Monitoring Network Traffic Using Traceroute on page 341](#)

Monitoring Hosts Using the J-Web Ping Host Tool

Purpose

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 27 on page 339](#).

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 27 on page 339](#) lists the fields.

Table 27: 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

Table 27: 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.	<ul style="list-style-type: none"> To suppress the display of the hop hostnames, select the check box. 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.	<ul style="list-style-type: none"> To set the DF bit, select the check box. 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.	<ul style="list-style-type: none"> To record and display the path of the packet, select the check box. 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	<p>Determines whether ping requests are routed by means of the routing table.</p> <p>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.</p>	<ul style="list-style-type: none"> To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. To route the ping requests using the routing table, clear the check box.

Related Documentation • [Monitoring Interface Status and Traffic](#)

Monitoring Network Traffic Using Traceroute

Purpose 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 28: 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		
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.

Table 28: Traceroute field summary (*continued*)

Field	Function	Your Action
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

CHAPTER 9

Configuration Statements for General Network Management and Monitoring

archive-sites

Syntax	<pre>archive-sites { <i>site-name</i>; }</pre>
Hierarchy Level	[edit accounting-options file filename]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format <i>router-name_log-filename_timestamp</i> .
Options	<i>site-name</i> —Any valid FTP URL to a destination. For information about specifying valid FTP URLs, see the Junos System Basics Configuration Guide .
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Archive Sites

class-usage-profile

Syntax	<pre>class-usage-profile <i>profile-name</i> { <i>file filename</i>; <i>interval minutes</i>; source-classes { <i>source-class-name</i>; } destination-classes { <i>destination-class-name</i>; } }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Create a class usage profile, which is used to log class usage statistics to a file in the <code>/var/log</code> directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has destination-class-usage configured.</p> <p>For information about configuring source classes, see the Junos Routing Protocols Configuration Guide. For information about configuring source class usage, see the Junos Network Interfaces Configuration Guide.</p>
Options	<p>profile-name—Name of the destination class profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">Configuring Class Usage Profiles

counters

Syntax	<code>counters { <i>counter-name</i>; }</code>
Hierarchy Level	[edit accounting-options filter-profile <i>profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the <code>/var/log</code> directory.
Options	<i>counter-name</i> —Name of the counter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Counters

destination-classes

Syntax	<code>destination-classes { <i>destination-class-name</i>; }</code>
Hierarchy Level	[edit accounting-options class-usage-profile <i>profile-name</i>]
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 destination classes for which statistics are collected.
Options	<i>destination-class-name</i> —Name of the destination class to include in the source class usage profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring a Class Usage Profile

fields (for Interface Profiles)

Syntax	<pre>fields { <i>field-name</i>; }</pre>
Hierarchy Level	[edit accounting-options interface-profile <i>profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Statistics to collect in an accounting-data log file for an interface.
Options	<p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none">• input-bytes—Input bytes• input-errors—Generic input error packets• input-multicast—Input packets arriving by multicast• input-packets—Input packets• input-unicast—Input unicast packets• output-bytes—Output bytes• output-errors—Generic output error packets• output-multicast—Output packets sent by multicast• output-packets—Output packets• output-unicast—Output unicast packets
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Interface Profile

file (Associating with a Profile)

Syntax	<code>file <i>filename</i>;</code>
Hierarchy Level	[edit accounting-options class-usage-profile <i>profile-name</i>], [edit accounting-options filter-profile <i>profile-name</i>], [edit accounting-options interface-profile <i>profile-name</i>], [edit accounting-options mib-profile <i>profile-name</i>], [edit accounting-options routing-engine-profile <i>profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. The [edit accounting-options mib-profile <i>profile-name</i>] hierarchy added in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series Switches.
Description	Specify the accounting log file associated with the profile.
Options	<i>filename</i> —Name of the log file. You must specify a filename already configured in the file statement at the [edit accounting-options] hierarchy level.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Interface Profile Configuring the Filter Profile Configuring the MIB Profile Configuring the Routing Engine Profile

file (Configuring a Log File)

Syntax	<pre>file <i>filename</i> { archive-sites { <i>site-name</i>; } files <i>number</i>; nonpersistent; size <i>bytes</i>; source-classes <i>time</i>; transfer-interval <i>minutes</i>; }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Specify a log file to be used for accounting data.
Options	<p><i>filename</i>—Name of the file in which to write accounting data.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Accounting-Data Log Files

files

Syntax	<code>files <i>number</i>;</code>
Hierarchy Level	[edit accounting-options file <i>filename</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the maximum number of log files to be used for accounting data.
Options	<i>number</i> —The maximum number of files. When a log file (for example, profilelog) reaches its maximum size, it is renamed profilelog.0 , then profilelog.1 , and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for <i>number</i> is 3 and the default value is 10.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Accounting-Data Log Files

filter-profile

Syntax	<pre>filter-profile <i>profile-name</i> { counters { counter-name; } file <i>filename</i>; interval <i>minutes</i>; }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Create a profile to filter and collect packet and byte count statistics and write them to a file in the <code>/var/log</code> directory. To apply the profile to a firewall filter, you include the accounting-profile statement at the [edit firewall filter <i>filter-name</i>] hierarchy level. For more information about firewall filters, see the Junos Network Interfaces Configuration Guide .
Options	<i>profile-name</i> —Name of the filter profile. 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	<ul style="list-style-type: none">Configuring the Filter Profile

interface-profile

Syntax	<pre>interface-profile <i>profile-name</i> { fields { <i>field-name</i>; } file <i>filename</i>; interval <i>minutes</i>; }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Create a profile to filter and collect error and packet statistics and write them to a file in the <code>/var/log</code> directory. You can specify an interface profile for either a physical or a logical interface.
Options	<p><i>profile-name</i>—Name of the interface profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">Configuring the Interface Profile

interval

Syntax	<code>interval <i>minutes</i>;</code>
Hierarchy Level	[edit accounting-options class-usage-profile <i>profile-name</i>], [edit accounting-options filter-profile <i>profile-name</i>], [edit accounting-options interface-profile <i>profile-name</i>], [edit accounting-options mib-profile <i>profile-name</i>], [edit accounting-options routing-engine-profile <i>profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. The [edit accounting-options mib-profile <i>profile-name</i>] hierarchy level added in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify how often statistics are collected for the accounting profile.
Options	<i>minutes</i> —Length of time between each collection of statistics. Range: 1 through 2880 minutes Default: 30 minutes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Interface Profile• Configuring the Filter Profile• Configuring the MIB Profile• Configuring the Routing Engine Profile

mib-profile

Syntax	<pre>mib-profile <i>profile-name</i> { file <i>filename</i>; interval <i>minutes</i>; object-names { <i>mib-object-name</i>; } operation <i>operation-name</i>; }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Create a MIB profile to collect selected MIB statistics and write them to a file in the <code>/var/log</code> directory.
Options	<p><i>profile-name</i>—Name of the MIB statistics profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the MIB Profile

object-names

Syntax	<code>object-names { <i>mib-object-name</i>; }</code>
Hierarchy Level	[edit accounting-options mib-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.
Options	<i>mib-object-name</i> —Name of a MIB object. You can specify more than one MIB object name.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the MIB Profile

operation

Syntax	<code>operation <i>operation-name</i>;</code>
Hierarchy Level	[edit accounting-options mib-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the name of the operation used to collect MIB statistics for an accounting-data log file.
Options	<i>operation-name</i> —Name of the operation to use. You can specify a get , get-next , or walk operation. Default: walk
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the MIB Profile

routing-engine-profile

Syntax	<pre>routing-engine-profile <i>profile-name</i> { fields { <i>field-name</i>; } file <i>filename</i>; interval <i>minutes</i>; }</pre>
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the <code>/var/log</code> directory.
Options	<i>profile-name</i> —Name of the Routing Engine statistics profile. 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	<ul style="list-style-type: none">Configuring the Routing Engine Profile

size

Syntax	<code>size bytes;</code>
Hierarchy Level	[edit accounting-options file <i>filename</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify attributes of an accounting-data log file.
Options	bytes —Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, profilelog) reaches its maximum size, it is renamed profilelog.0 , then profilelog.1 , and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded. Syntax: <i>x</i> to specify bytes, <i>xk</i> to specify KB, <i>xm</i> to specify MB, <i>xg</i> to specify GB Range: 256 KB through 1 GB
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Maximum Size of the File

source-classes

Syntax	<pre>source-classes { <i>source-class-name</i>; }</pre>
Hierarchy Level	[edit accounting-options class-usage-profile <i>profile-name</i>]
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 source classes for which statistics are collected.
Options	source-class-name —Name of the source class to include in the class usage profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring a Class Usage Profile

start-time

Syntax	<code>start-time <i>time</i>;</code>
Hierarchy Level	[edit accounting-options file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the start time for transfer of an accounting-data log file.
Options	<i>time</i> —Start time for file transfer. Syntax: <i>YYYY-MM-DD.hh:mm</i>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Start Time for File Transfer

transfer-interval

Syntax	<code>transfer-interval <i>minutes</i>;</code>
Hierarchy Level	[edit accounting-options file <i>filename</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.
Options	<i>minutes</i> —Time the file remains open and receives new statistics before it is closed and transferred to an archive site. Range: 5 through 2880 minutes Default: 30 minutes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the Transfer Interval of the File

CHAPTER 10

Operational Commands for General Network Management and Monitoring

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.

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 QFX3000 QFabric switch.

Options none—(Optional) Display packet headers transmitted through **fxp0**. On a TX Matrix Plus router, display packet headers transmitted through **em0**.

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

absolute-sequence—(Optional) Display absolute TCP sequence numbers.

count *count*—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The monitor traffic command quits automatically after displaying the number of packets specified.

interface *interface-name*—(Optional) Specify the interface on which the **monitor traffic** command displays packet data. If no interface is specified, the **monitor traffic** command displays packet data arriving on the lowest-numbered interface.

layer2-headers—(Optional) Display the link-level header on each line.

matching *matching*—(Optional) Display packet headers that match a regular expression. Use matching expressions to define the level of detail with which the **monitor traffic** command filters and displays packet data.

no-domain-names—(Optional) Suppress the display of the domain portion of hostnames. With the **no-domain-names** option enabled, the **monitor traffic** command displays only **team** for the hostname **team.company.net**.

no-promiscuous—(Optional) Do not put the interface into promiscuous mode.

no-resolve—(Optional) Suppress reverse lookup of the IP addresses.

no-timestamp—(Optional) Suppress timestamps on displayed packets.

print-ascii—(Optional) Display each packet in ASCII format.

print-hex—(Optional) Display each packet, except the link-level header, in hexadecimal format.

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 29 on page 362](#).

Table 29: Match Conditions for the monitor traffic Command

Match Type	Condition	Description
Entity	host [<i>address</i> <i>hostname</i>]	Matches packets that contain the specified address or hostname. The protocol match conditions arp , ip , or rarp , or any of the directional match conditions can be prepended to the host match condition.
	net <i>address</i>	Matches packets with source or destination addresses containing the specified network address.
	net <i>address mask mask</i>	Matches packets containing the specified network address and subnet mask.
	port (<i>port-number</i> <i>port-name</i>)	Matches packets containing the specified source or destination TCP or UDP port number or port name. In place of the numeric port address, you can specify a text synonym, such as bgp (179), dhcp (67), or domain (53) (the port numbers are also listed).
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 <i>value</i>	Matches packets shorter than or equal to the specified value, in bytes.
	greater <i>value</i>	Matches packets longer than or equal to the specified value, in bytes.

Table 29: 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 igmp 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.
	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 30 on page 363](#).

Table 30: 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.

Table 30: Logical Operators for the monitor traffic Command (*continued*)

Logical Operator (Highest to Lowest Precedence)	Description
&&	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 31 on page 365](#).



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 29 on page 362](#).
- 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 31: 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.
=	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 366](#)
[monitor traffic detail count on page 366](#)
[monitor traffic extensive \(Absolute Sequence\) on page 366](#)
[monitor traffic extensive \(Relative Sequence\) on page 366](#)
[monitor traffic extensive count on page 366](#)
[monitor traffic interface on page 367](#)
[monitor traffic matching on page 367](#)
[monitor traffic \(TX Matrix Plus Router\) on page 367](#)
[monitor traffic \(QFX3500 Switch\) on page 368](#)

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   user@host> monitor traffic detail count 2
count                     listening on fxp0
                             04:38:16.265864 In my-server.home.net.1295 > my-server.work.net.telnet: . ack
                             4122529971 win 17678 (DF) (ttl 121, id 6812)
                             04:38:16.265926
                             Out my-server.work.net.telnet.telnet > my-server.home.net.1295: P 1:38(37) ack 0
                             win 17680 (DF) [tos 0x10] (ttl 6)

monitor traffic          user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
extensive                matching "tcp" absolute-sequence
(Absolute Sequence)      listening on fxp0
                             In 207.17.136.193.179 > 192.168.4.227.1024: . 4042780859:4042780859(0)
                             ack 1845421797 win 16384 <nop,nop,timestamp 4935628 965951> [tos 0xc0] (ttl )
                             In 207.17.136.193.179 > 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 > 207.17.136.193.179:
                             P 1845421797:1845421852(55) ack 4042780912 win 16384 <nop,nop,timestamp 965951
                             4935628>: BGP [|BGP UPDAT)
                             ...

monitor traffic          user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
extensive                matching "tcp"
(Relative Sequence)      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 207.17.136.193.179 > 192.168.4.227.1024: P 4042775817:4042775874(57)
                             ack 1845416593 win 16384 <nop,nop,timestamp 4935379 965690>: BGP [|BGP UPDAT)
                             ...

monitor traffic          user@host> monitor traffic extensive count 5 no-domain-names no-resolve
extensive count          listening on fxp013:18:17.406933
                             In 192.168.4.206.2723610880 > 172.17.28.8.2049:
                             40 null (ttl 64, id 38367)13:18:17.407577
                             In 172.17.28.8.2049 > 192.168.4.206.2723610880:
                             reply ok 28 null (ttl 61, id 35495)13:18:17.541140
                             In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
                             0000 0100 0000 0000
                             0000 0000 0000 0000
                             0000 0000 0000 0000
                             0000 0000 0000 0000
                             0000 0000 0000 0000
                             0000 0000 000013:18:17.591513

```

```
In 172.24.248.156.4139 > 192.168.4.210.23:
3556964918:3556964918(0)
ack 295526518 win 17601 (DF)
(ttl 121, id 14)13:18:17.591568
Out 192.168.4.210.23 >
172.24.248.156.4139: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]
(ttl 64, id 52376)
```

monitor traffic interface

```
user@host> monitor traffic interface fxp0
listening on fxp0.0
18:17:28.800650 In server.home.net.723 > host1-0.lab.home.net.log
18:17:28.800733 Out host2-0.lab.home.net.login > server.home.net.7
18:17:28.817813 In host30.lab.home.net.syslog > host40.home0
18:17:28.817846 In host30.lab.home.net.syslog > host40.home0
...
```

monitor traffic matching

```
user@host> monitor traffic matching "net 192.168.1.0/24"
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes

Reverse lookup for 192.168.1.255 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use no-resolve to avoid reverse lookups on IP addresses.
```

```
21:55:54.003511 In IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003585 Out IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003864 In arp who-has 192.168.1.17 tell 192.168.1.9
...
```

monitor traffic (TX Matrix Plus Router)

```
user@host> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em0, capture size 96 bytes
04:11:59.862121 Out IP truncated-ip - 25 bytes missing!
summit-em0.englab.juniper.net.syslog > sv-log-01.englab.juniper.net.syslog:
SYSLOG kernel.info, length: 57
04:11:59.862303
Out IP truncated-ip - 25 bytes missing!
summit-em0.englab.juniper.net.syslog >
sv-log-02.englab.juniper.net.syslog: SYSLOG kernel.info, length: 57
04:11:59.923948
In IP aj-em0.englab.juniper.net.65235 >
summit-em0.englab.juniper.net.telnet: .
ack 1087492766 win 33304 <nop,nop,timestamp 42366734 993490>
04:11:59.923983 Out IP truncated-ip - 232 bytes missing!
summit-em0.englab.juniper.net.telnet > aj-em0.englab.juniper.net.65235: P
1:241(240) ack 0 win 33304
<nop,nop,timestamp 993590 42366734>
04:12:00.022900
In IP aj-em0.englab.juniper.net.65235 >
summit-em0.englab.juniper.net.telnet: . ack 241 win 33304 <nop,nop,timestamp
42366834 993590>
04:12:00.141204
In IP truncated-ip - 40 bytes missing!
```

```

ipg-lnx-shell11.juniper.net.46182 > summit-em0.englab.juniper.net.telnet: P
2950530356:2950530404(48) ack 485494987 win 63712
<nop,nop,timestamp 1308555294 987086>
04:12:00.141345
Out IP summit-em0.englab.juniper.net.telnet >
ipg-lnx-shell11.juniper.net.46182: P 1:6(5)
ack 48 win 33304
<nop,nop,timestamp 993809 1308555294>
04:12:00.141572
In IP ipg-lnx-shell11.juniper.net.46182 >
summit-em0.englab.juniper.net.telnet: .
ack 6 win 63712
<nop,nop,timestamp 1308555294 993809>
04:12:00.141597
Out IP summit-em0.englab.juniper.net.telnet >
ipg-lnx-shell11.juniper.net.46182: P 6:10(4) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.141821
In IP ipg-lnx-shell11.juniper.net.46182 >
summit-em0.englab.juniper.net.telnet: .
ack 10 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.141837 Out IP truncated-ip - 2 bytes missing!
summit-em0.englab.juniper.net.telnet >
ipg-lnx-shell11.juniper.net.46182: P 10:20(10) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.142072
In IP ipg-lnx-shell11.juniper.net.46182 >
summit-em0.englab.juniper.net.telnet: . ack 20 win 63712
<nop,nop,timestamp 1308555294 993810>
04:12:00.142089 Out IP summit-em0.englab.juniper.net.telnet >
ipg-lnx-shell11.juniper.net.46182: P 20:28(8) ack 48 win 33304 <nop,nop,timestamp
993810 1308555294>
04:12:00.142321
In IP ipg-lnx-shell11.juniper.net.46182 >
summit-em0.englab.juniper.net.telnet: .
ack 28 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.142337
Out IP truncated-ip - 1 bytes missing!
summit-em0.englab.juniper.net.telnet >
ipg-lnx-shell11.juniper.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.lab4.juniper.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.lab4.juniper.net.ssh >
172.22.16.246.telefinder: P 132:328(196) ack 1 win 65535
...

```


ping

Syntax `ping host`
 `<bypass-routing>`
 `<count requests>`
 `<detail>`
 `<do-not-fragment>`
 `<inet | inet6>`
 `<interface source-interface>`
 `<interval seconds>`
 `<logical-system (all | logical-system-name)>`
 `<loose-source value>`
 `<no-resolve>`
 `<pattern string>`
 `<rapid>`
 `<record-route>`
 `<routing-instance routing-instance-name>`
 `<size bytes>`
 `<source source-address>`
 `<strict >`
 `<strict-source value.>`
 `<tos type-of-service>`
 `<ttl value>`
 `<verbose>`
 `<wait seconds>`

Syntax (QFX Series) `ping host`
 `<bypass-routing>`
 `<count requests>`
 `<detail>`
 `<do-not-fragment>`
 `<inet>`
 `<interface source-interface>`
 `<interval seconds>`
 `<loose-source value>`
 `<mac-address mac-address>`
 `<no-resolve>`
 `<pattern string>`
 `<rapid>`
 `<record-route>`
 `<routing-instance routing-instance-name>`
 `<size bytes>`
 `<source source-address>`
 `<strict>`
 `< strict-source value>`
 `<tos type-of-service>`
 `<ttl value>`
 `<verbose>`
 `<wait seconds>`

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

Description 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. Type 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.

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.

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) Delay, in seconds, after sending the last packet. If this option is not specified, the default delay is 10 seconds. If this option is used without the count option, a default count of 5 packets is used.

Required Privilege Level

network

Related Documentation

- [Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages](#)

List of Sample Output

[ping hostname on page 372](#)
[ping hostname size count on page 372](#)
[ping hostname rapid on page 372](#)

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 skye
PING skye.net (192.168.169.254): 56 data bytes
64 bytes from 192.168.169.254: icmp_seq=0 ttl=253 time=1.028 ms
64 bytes from 192.168.169.254: icmp_seq=1 ttl=253 time=1.053 ms
64 bytes from 192.168.169.254: icmp_seq=2 ttl=253 time=1.025 ms
64 bytes from 192.168.169.254: icmp_seq=3 ttl=253 time=1.098 ms
64 bytes from 192.168.169.254: icmp_seq=4 ttl=253 time=1.032 ms
64 bytes from 192.168.169.254: icmp_seq=5 ttl=253 time=1.044 ms
^C [abort]

ping hostname user@host> ping skye size 200 count 5
size count PING skye.net (192.168.169.254): 200 data bytes
208 bytes from 192.168.169.254: icmp_seq=0 ttl=253 time=1.759 ms
208 bytes from 192.168.169.254: icmp_seq=1 ttl=253 time=2.075 ms
208 bytes from 192.168.169.254: icmp_seq=2 ttl=253 time=1.843 ms
208 bytes from 192.168.169.254: icmp_seq=3 ttl=253 time=1.803 ms
208 bytes from 192.168.169.254: icmp_seq=4 ttl=253 time=17.898 ms

--- skye.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.759/5.075/17.898 ms

ping hostname rapid user@host> ping skye rapid
PING skye.net (192.168.169.254): 56 data bytes
!!!!
--- skye.net 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

```

show snmp mib

Syntax	<code>show snmp mib (get get-next walk) (ascii decimal) <i>object-id</i></code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>ascii and decimal options introduced in Junos OS Release 9.6.</p> <p>ascii and decimal options introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.
Options	<p>get—Retrieve and display one or more SNMP object values.</p> <p>get-next—Retrieve and display the next SNMP object values.</p> <p>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.</p> <p>ascii—Display the SNMP object's string indices as an ASCII-key representation.</p> <p>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.</p> <p>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.</p>
Required Privilege Level	snmp—To view this statement in the configuration.
List of Sample Output	<p>show snmp mib get on page 374</p> <p>show snmp mib get (Multiple Objects) on page 374</p> <p>show snmp mib get-next on page 374</p> <p>show snmp mib get-next (Specify an OID) on page 374</p> <p>show snmp mib walk on page 374</p> <p>show snmp mib walk (QFX Series) on page 374</p> <p>show snmp mib walk decimal on page 374</p> <p>show snmp mib walk (ASCII) on page 374</p> <p>show snmp mib walk (Multiple Indices) on page 374</p> <p>show snmp mib walk decimal (Multiple Indices) on page 375</p>
Output Fields	Table 32 on page 374 describes the output fields for the show snmp mib command. Output fields are listed in the approximate order in which they appear.

Table 32: show snmp mib Output Fields

Field Name	Field Description
<i>name</i>	Object name and numeric instance value.
<i>object value</i>	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      user@host> show snmp mib get ?sysObjectID.0 sysUpTime.0?
(Multiple Objects)     sysObjectID.0 = jnxProductNameM20
                        sysUpTime.0 = 1640992

show snmp mib          user@host> show snmp mib get-next jnxMibs
get-next               jnxBoxClass.0 = jnxProductLineM20.0

show snmp mib          user@host> show snmp mib get-next 1.3.6.1
get-next (Specify an   sysDescr.0 = Juniper Networks, Inc. m20 internet router, kernel
OID)                   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     user@switch> show snmp mib walk system
(QFX Series)           sysDescr.0 = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
                        11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
                        sysObjectID.0 = jnxProductQFX3500
                        sysUpTime.0 = 138980301
                        sysContact.0 = System Contact
                        sysName.0 = LabQFX3500
                        sysLocation.0 = Lab
                        sysServices.0 = 4

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

show snmp mib walk     show snmp mib walk ascii jnxUtilData
(ASCII)               jnxUtilCounter32Value."fred" = 100

show snmp mib walk     show snmp mib walk ascii jnxFWCounterByteCount
(Multiple Indices)     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
.....
```

traceroute

Syntax	<code>traceroute host</code> <code><as-number-lookup></code> <code><bypass-routing></code> <code><clns></code> <code><gateway address></code> <code><inet inet6></code> <code><interface interface-name></code> <code><logical system (all logical-system-name)></code> <code><mpls (ldp FEC address rsvp label-switched-path-name)></code> <code><no-resolve></code> <code><routing-instance routing-instance-name></code> <code><source source-address></code> <code><tos value></code> <code><ttl value></code> <code><wait seconds></code>
Syntax (QFX Series)	<code>traceroute host</code> <code><as-number-lookup></code> <code><bypass-routing></code> <code><gateway address></code> <code><inet></code> <code><interface interface-name></code> <code><monitor host></code> <code><no-resolve></code> <code><routing-instance routing-instance-name></code> <code><source source-address></code> <code><tos value></code> <code><ttl value></code> <code><wait seconds></code>
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. Command introduced in Junos OS Release 11.1 for the QFX Series.
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	<i>host</i> —IP address or name of remote host. <i>as-number-lookup</i> —(Optional) Display the autonomous system (AS) number of each intermediate hop on the path from the host to the destination. <i>bypass-routing</i> —(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. <i>clns</i> —(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.

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.

routing-instance routing-instance-name—(Optional) Name of the routing instance for the `traceroute` attempt.

source source-address—(Optional) Source address of the outgoing `traceroute` packets.

tos value—(Optional) Value to include in the IP type-of-service (ToS) field. The range of values is 0 through 255.

ttl value—(Optional) Maximum time-to-live value to include in the `traceroute` request. The range of values is 0 through 128.

wait seconds—(Optional) Maximum time to wait for a response to the `traceroute` request.

Required Privilege Level network

Related Documentation

- `traceroute monitor`

List of Sample Output [traceroute on page 378](#)
[traceroute as-number-lookup host on page 378](#)
[traceroute no-resolve on page 378](#)
[traceroute \(Between CE Routers, Layer 3 VPN\) on page 378](#)
[traceroute \(Through an MPLS LSP\) on page 378](#)

Output Fields [Table 33 on page 377](#) describes the output fields for the `traceroute` command. Output fields are listed in the approximate order in which they appear.

Table 33: traceroute Output Fields

Field Name	Field Description
<code>traceroute to</code>	IP address of the receiver.
<code>hops max</code>	Maximum number of hops allowed.

Table 33: traceroute Output Fields (*continued*)

Field Name	Field Description
byte packets	Size of packets being sent.
<i>number-of-hops</i>	Number of hops from the source to the named router or switch.
<i>router-name</i>	Name of the router or switch for this hop.
<i>address</i>	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 green.company.net (10.156.169.254), 30 hops max, 40 byte packets
 1 blue23 (10.168.1.254)  2.370 ms  2.853 ms  0.367 ms
 2 red14  (10.168.255.250) 0.778 ms  2.937 ms  0.446 ms
 3 yellow (10.156.169.254) 7.737 ms  89.905 ms  0.834 ms

```

```

traceroute      user@host> traceroute as-number-lookup 10.100.1.1
as-number-lookup traceroute to 10.100.1.1 (10.100.1.1), 30 hops max, 40 byte packets
host             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

```

```

traceroute no-resolve user@host> traceroute santacruz no-resolve
traceroute to green.company.net (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 (Between user@host> traceroute vpn09
CE Routers, Layer 3 traceroute to vpn09.skybank.net (10.255.14.179), 30 hops max, 40
VPN)                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 vpn09.skybank.net (10.255.14.179) 0.783 ms 0.716 ms 0.686

```

```

traceroute      user@host> traceroute mpls1
(Through an MPLS traceroute to 10.168.1.224 (10.168.1.224), 30 hops max, 40 byte packets
LSP)           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 mpls5-1o0.company.net (10.168.1.224) 0.420 ms 0.394 ms 0.401 ms

```