



Network Management and Monitoring Feature Guide for QFabric Systems

Release

14.1X53



Modified: 2015-08-27

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

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

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

Network Management and Monitoring Feature Guide for QFabric Systems
14.1X53
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xvii
	Documentation and Release Notes	xvii
	Supported Platforms	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Overview	
Chapter 1	Network Management	3
	Understanding Device and Network Management Features	3
	Understanding Network Management Implementation on the QFabric System	6
	Understanding Telnet on the QFabric System	7
	Understanding Tracing and Logging Operations	7
Chapter 2	Automation Scripts	11
	Understanding Automation Scripts Support	11
	How Commit Scripts Work	12
	Commit Script Input	13
	Commit Script Output	14
	Commit Scripts and the Junos OS Commit Model	15
	Standard Commit Model	15
	Commit Model with Commit Scripts	15
	Avoiding Potential Conflicts When Using Multiple Commit Scripts	17
	Overview of Generating Persistent or Transient Configuration Changes	18
	Differences Between Persistent and Transient Changes	19
	Interaction of Configuration Changes and Configuration Groups	22
	Tag Elements and Templates for Generating Changes	22
	Required Boilerplate for Commit Scripts	23
	How Op Scripts Work	24
	Required Boilerplate for Op Scripts	25
Chapter 3	Fabric OAM	29
	Overview of Internal Fabric Monitoring	29

Chapter 4	Junos Space	31
	Understanding Junos Space Support	31
	Preparing the Device for Junos Space Management	32
Chapter 5	sFlow Technology	35
	Overview of sFlow Technology	35
Chapter 6	SNMP	39
	Understanding the Implementation of SNMP	39
	Understanding the Implementation of SNMP on the QFabric System	42
	Fabric Chassis MIB	44
	Utility MIB	48
	SNMPv3 Overview	49
	Minimum SNMPv3 Configuration on a Device Running Junos OS	50
	Understanding RMON	51
	RMON Overview	51
	Alarm Thresholds and Events	52
	RMON MIB Event, Alarm, Log, and History Control Tables	53
	Understanding Health Monitoring	55
	SNMP MIBs Support	56
	MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	56
	MIBs Supported on QFabric Systems	66
	SNMP Traps Support	72
	SNMP Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	72
	SNMPv1 Traps	73
	SNMPv2 Traps	77
	SNMP Traps Supported on QFabric Systems	81
	MIB Objects for the QFX Series	85
	QFX Series Standalone Switches	85
	QFabric Systems	85
	QFabric System QFX3100 Director Device	86
	QFabric System QFX3008-I Interconnect Device	86
	QFabric System QFX3600-I Interconnect Device	86
	QFabric System Node Devices	87
Chapter 7	System Logging	89
	Overview of Junos OS System Log Messages	89
	Overview of Single-Chassis System Logging Configuration	89
	Understanding the Implementation of System Log Messages on the QFabric System	91
Part 2	Configuring	
Chapter 8	Network Management	95
	Configuring Console and Auxiliary Port Properties	95
	Configuring SSH Service for Remote Access to the Router or Switch	96
	Configuring the Root Login Through SSH	97
	Configuring the SSH Protocol Version	97

	Configuring the Client Alive Mechanism	97
	Configuring Telnet Service for Remote Access to a Switch	98
Chapter 9	Automation Scripts	99
	Controlling the Execution of Commit Scripts	99
	Enabling Commit Scripts to Execute	99
	Removing Commit Scripts from the Configuration	100
	Deactivating Commit Scripts	101
	Activating Inactive Commit Scripts	101
Chapter 10	Fabric OAM	103
	Configuring a Fabric Maintenance Association	103
	Configuring Flow Specifications	104
	Configuring a Unicast Ethernet Flow Specification	105
	Configuring a Unicast Ethernet IPv4 Flow Specification	106
	Configuring a Multicast IPv4 Flow Specification	107
	Configuring a Multicast VLAN Flood Flow Specification	107
	Example: Configuring Internal Fabric OAM Monitoring	108
Chapter 11	sFlow Technology	115
	Configuring sFlow Technology	115
	Example: Monitoring Network Traffic Using sFlow Technology	116
Chapter 12	SNMP	121
	Configuring SNMP	121
	Configuring the SNMP Community String	125
	Configuring SNMP Trap Groups	126
	Adding a Group of Clients to an SNMP Community	127
	Configuring the Interfaces on Which SNMP Requests Can Be Accepted	128
	Configuring MIB Views	129
	Configuring RMON Alarms and Events	130
	Configuring SNMP	131
	Configuring an Event	131
	Configuring an Alarm	132
	Configuring Health Monitoring	132
	Creating SNMPv3 Users	133
	Configuring Access Privileges for a Group	134
	Assigning a Security Name to a Group	136
	Configuring SNMPv3 Traps on a Device Running Junos OS	137
	Configuring SNMP Informs	138
	Example: Configuring SNMP	139
Chapter 13	System Log Messages	143
	Junos OS Minimum System Logging Configuration	144
	Junos OS System Log Configuration Statements	144
	Adding a Text String to System Log Messages Directed to a Remote Destination	145
	Directing System Log Messages to a Log File	146
	Directing System Log Messages to a Remote Machine	147
	Directing System Log Messages to a User Terminal	147
	Directing System Log Messages to the Console	148

	Disabling the System Logging of a Facility	148
	Displaying a Log File from a Single-Chassis System	149
	Including Priority Information in System Log Messages	150
	Including the Year or Millisecond in Timestamps	151
	Logging Messages in Structured-Data Format	152
	Interpreting Messages Generated in Structured-Data Format	153
	Interpreting Messages Generated in Standard Format	156
	Specifying Log File Size, Number, and Archiving Properties	157
	Specifying the Facility and Severity of Messages to Include in the Log	158
	Junos OS System Logging Facilities and Message Severity Levels	159
	Default Facilities for System Log Messages Directed to a Remote Destination	160
	Alternate Facilities for System Log Messages Directed to a Remote Destination	161
	Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination	162
	Using Regular Expressions to Refine the Set of Logged Messages	164
	Examples: Configuring System Logging	166
	Examples: Assigning an Alternative Facility	168
	Example: Configuring System Log Messages	169
Part 3	Monitoring and Troubleshooting	
Chapter 14	Routine Monitoring Using the CLI	175
	Displaying a Log File from a Single-Chassis System	175
	Monitoring Traffic Through the Router or Switch	176
	Displaying Real-Time Statistics About All Interfaces on the Router or Switch	176
	Displaying Real-Time Statistics About an Interface on the Router or Switch	177
	Monitoring RMON MIB Tables	179
	Monitoring SNMP	179
	Monitoring System Log Messages	181
	Pinging Hosts	182
	Tracing SNMP Activity on a Device Running Junos OS	183
	Configuring the Number and Size of SNMP Log Files	184
	Configuring Access to the Log File	184
	Configuring a Regular Expression for Lines to Be Logged	185
	Configuring the Trace Operations	185
	Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage	186
	Displaying Commit Script Output	188
Chapter 15	Troubleshooting Overview	191
	Understanding Troubleshooting Resources	191
	Troubleshooting Overview	193
	Automation Enhancements Frequently Asked Questions	195
	Who Should You Contact If You Have Problems with Loading, Installing or Updating Libraries?	196
	Who Should You Contact If You Have Problems with Puppet for Junos OS?	196

	Who Should You Contact If You Have Problems with Chef for Junos OS?	196
	What Happens to the User Partition If You Downgrade a Device That Is Running the Junos Automation Enhancements Software Bundle to a Device That Is Running a Different Software Bundle?	196
	How Do You Recover Junos OS Binaries That You Have Deleted?	196
	How Do You Recover from a System Crash?	196
	How Can You Verify That a Device Is Running a Junos Automation Enhancements Software Bundle?	196
Chapter 16	Troubleshooting Procedures	199
	Recovering from a Failed Software Installation	199
	Loading a Previous Configuration File	201
	Reverting to the Default Factory Configuration	201
	Reverting to the Rescue Configuration	202
	Recovering the Root Password	202
	Troubleshooting a Deprecated Network Analytics Configuration	204
Part 4	Configuration Statements and Operational Commands	
Chapter 17	Configuration Statements for Network Management	207
	connection-limit	208
	destination-override	209
	no-remote-trace	209
	protocol-version	210
	rate-limit	211
	ssh	212
	telnet	213
	tracing	214
Chapter 18	Configuration Statements for Automation Scripts	215
	allow-transients	216
	apply-macro	217
	checksum	218
	command	219
	commit	220
	description	221
	direct-access	221
	file (Commit Scripts)	222
	file (Op Scripts)	223
	no-allow-url	224
	op	225
	optional	226
	refresh (Commit Scripts)	227
	refresh (Op Scripts)	228
	refresh-from (Commit Scripts)	229
	refresh-from (Op Scripts)	230
	scripts	231
	source (Commit Scripts)	233
	source (Op Scripts)	234

Chapter 19	Configuration Statements for Fabric OAM	235
	ethernet-frame-size	236
	fabric (OAM)	237
	fabric-maintenance-associations	239
	fabric-maintenance-end-points	240
	flow-specs	241
	unicast-ethernet-ipv4	243
	multicast-ipv4	245
	multicast-vlan-flood	246
	unicast-ethernet	247
Chapter 20	Configuration Statements for sFlow Technology	249
	agent-id	249
	collector (sFlow Technology)	250
	interfaces (sFlow)	251
	polling-interval	252
	sample-rate	253
	sflow	254
	source-ip	255
	traceoptions (sFlow Technology)	256
	udp-port	257
Chapter 21	Configuration Statements for SNMP	259
	access (SNMP)	262
	address (SNMP)	262
	address-mask	263
	agent-address	263
	alarm (SNMP RMON)	264
	authentication-md5	265
	authentication-none	266
	authentication-password	267
	authentication-sha	268
	authorization	269
	bucket-size	270
	categories	271
	client-list	271
	client-list-name	272
	clients	272
	commit-delay	273
	community (SNMP)	274
	community (RMON)	275
	community-name (SNMP)	276
	contact	277
	description (SNMP)	278
	description (RMON)	279
	destination-port (SNMP)	279
	engine-id	280
	event	281
	falling-event-index (RMON)	282

falling-threshold (Health Monitor)	283
falling-threshold (RMON)	284
falling-threshold-interval	285
filter-duplicates	285
filter-interfaces	286
group (Associating a Security Name)	287
group (Configuring Access Privileges)	288
health-monitor	289
history	290
interface (SNMP)	291
interface (RMON)	292
interval (Health Monitor)	293
interval (RMON)	294
local-engine	295
location	296
logical-system (SNMP)	297
message-processing-model	298
name	298
nonvolatile	299
notify	300
notify-filter (Applying to the Management Target)	301
notify-filter (Configuring the Profile Name)	301
notify-view	302
oid	302
oid (SNMPv3)	303
owner	304
parameters	305
port (SNMP)	305
privacy-3des	306
privacy-aes128	307
privacy-des	308
privacy-none	309
privacy-password	310
read-view	311
remote-engine	312
request-type	313
retry-count (SNMPv3)	314
rising-event-index	315
rising-threshold (Health Monitor)	316
rising-threshold (RMON)	317
rmon	318
routing-instance (SNMP)	319
sample-type	320
security-level (Defining Access Privileges)	321
security-level (Generating SNMP Notifications)	322
security-model (Access Privileges)	323
security-model (Group)	324
security-model (SNMP Notifications)	325
security-name (Community String)	326

security-name (Security Group)	327
security-name (SNMP Notifications)	328
security-to-group	329
snmp	330
snmp-community	334
source-address (SNMP)	335
startup-alarm	336
syslog-subtag	337
tag (Configuring Notification Targets)	337
tag (Configuring the SNMP Community)	338
tag-list	338
target-address	339
target-parameters	340
targets	341
timeout	341
traceoptions (SNMP)	342
trap-group	344
trap-options	345
type (RMON Notification)	346
type (SNMPv3)	347
user	347
usm	348
v3	350
vacm	352
variable	353
version	354
view (Configuring a MIB View)	355
view (Associating MIB View with a Community)	356
write-view	356
Chapter 22 Configuration Statements for System Log Messages	357
archive (All System Log Files)	358
archive (Individual System Log File)	360
archive (QFabric System)	361
console (System Logging)	362
explicit-priority	363
facility-override	364
file (QFabric System)	365
file (System Logging)	366
files	367
host (System)	368
log-prefix (System)	370
match	370
size (System)	371
structured-data	372
syslog (System)	373
syslog (QFabric System)	375
time-format	376
user (System Logging)	377

Chapter 23	Monitoring Commands	379
	clear sflow collector statistics	380
	clear snmp history	381
	clear snmp statistics	382
	monitor traffic	384
	ping	394
	ping fabric multicast-flow	398
	ping fabric unicast-flow	400
	request snmp spoof-trap	403
	request snmp utility-mib clear instance	409
	request snmp utility-mib set instance	410
	show oam fabric flow-specification	411
	show oam fabric interfaces	414
	show log	416
	show sflow	419
	show sflow collector	421
	show sflow interface	422
	show snmp health-monitor	424
	show snmp inform-statistics	429
	show snmp mib	431
	show snmp rmon	434
	show snmp rmon history	438
	show snmp statistics	439
	show snmp v3	443
	traceroute fabric unicast-flow	446

List of Figures

Part 1	Overview	
Chapter 2	Automation Scripts	11
	Figure 1: Commit Script Input and Output	13
	Figure 2: Standard Commit Model	15
	Figure 3: Commit Model with Commit Scripts Added	16
	Figure 4: Configuration Evaluation by Multiple Commit Scripts	18
	Figure 5: Op Script Input and Output	25
Chapter 6	SNMP	39
	Figure 6: SNMP Communication Flow	41
	Figure 7: Setting Thresholds	52
Part 2	Configuring	
Chapter 11	sFlow Technology	115
	Figure 8: sFlow Technology Monitoring System	117
Chapter 12	SNMP	121
	Figure 9: Inform Request and Response	138

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xix
Part 1	Overview	
Chapter 1	Network Management	3
	Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600	3
Chapter 2	Automation Scripts	11
	Table 4: Differences Between Persistent and Transient Changes	20
Chapter 6	SNMP	39
	Table 5: Fabric Chassis MIB Tables and Objects	45
	Table 6: Fabric Chassis MIB SNMPv2 Traps	47
	Table 7: RMON Event Table	53
	Table 8: RMON Alarm Table	53
	Table 9: jnxRmon Alarm Table	54
	Table 10: RMON History Control Table	54
	Table 11: Monitored Object Instances	56
	Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	57
	Table 13: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	62
	Table 14: Standard MIBs Supported on QFabric Systems	66
	Table 15: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems	70
	Table 16: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	73
	Table 17: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	75
	Table 18: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	77
	Table 19: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series	79
	Table 20: Standard SNMPv2 Traps Supported on QFabric Systems	82
	Table 21: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems	83
Part 2	Configuring	
Chapter 10	Fabric OAM	103

	Table 22: Fabric OAM Configuration Elements	110
Chapter 13	System Log Messages	143
	Table 23: Minimum Configuration Statements for System Logging	144
	Table 24: Fields in Structured-Data Messages	153
	Table 25: Facility and Severity Codes in the priority-code Field	155
	Table 26: Fields in Standard-Format Messages	156
	Table 27: Junos OS System Logging Facilities	159
	Table 28: System Log Message Severity Levels	160
	Table 29: Default Facilities for Messages Directed to a Remote Destination	160
	Table 30: Facilities for the facility-override Statement	161
	Table 31: Regular Expression Operators for the match Statement	164
Part 3	Monitoring and Troubleshooting	
Chapter 14	Routine Monitoring Using the CLI	175
	Table 32: Output Control Keys for the monitor interface Command	178
	Table 33: SNMP Tracing Flags	185
	Table 34: Commit Script Configuration and Operational Mode Commands	188
Chapter 15	Troubleshooting Overview	191
	Table 35: Troubleshooting Resources on the QFX and OCX Series	191
	Table 36: Troubleshooting on the QFX Series	193
Part 4	Configuration Statements and Operational Commands	
Chapter 23	Monitoring Commands	379
	Table 37: Match Conditions for the monitor traffic Command	386
	Table 38: Logical Operators for the monitor traffic Command	387
	Table 39: Arithmetic and Relational Operators for the monitor traffic Command	389
	Table 40: ping fabric multicast-flow Output Fields	398
	Table 41: ping fabric unicast-flow Output Fields	401
	Table 42: show oam fabric flow-specification Output Fields	411
	Table 43: show oam fabric interfaces Output Fields	414
	Table 44: show sflow Output Fields	419
	Table 45: show sflow collector Output Fields	421
	Table 46: show sflow interface Output Fields	422
	Table 47: show snmp health-monitor Output Fields	424
	Table 48: show snmp inform-statistics Output Fields	429
	Table 49: show snmp mib Output Fields	432
	Table 50: show snmp rmon Output Fields	434
	Table 51: show snmp statistics Output Fields	439
	Table 52: show snmp v3 Output Fields	444
	Table 53: traceroute fabric unicast-flow Output Fields	447

About the Documentation

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

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

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

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

Supported Platforms

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

- QFabric System

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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


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

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

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

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xix defines notice icons used in this guide.

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide 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 CLI User 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>
Text like this	Represents names of configuration statements, commands, files, and directories; 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.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

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

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Network Management on page 3](#)
- [Automation Scripts on page 11](#)
- [Fabric OAM on page 29](#)
- [Junos Space on page 31](#)
- [sFlow Technology on page 35](#)
- [SNMP on page 39](#)
- [System Logging on page 89](#)

CHAPTER 1

Network Management

- [Understanding Device and Network Management Features on page 3](#)
- [Understanding Network Management Implementation on the QFabric System on page 6](#)
- [Understanding Telnet on the QFabric System on page 7](#)
- [Understanding Tracing and Logging Operations on page 7](#)

Understanding Device and Network Management Features

After you install a QFX Series product, OCX Series device, or EX4600 switch in your network, you need to manage the device. The products support features that you use to manage the device within the network, including the management of configuration, system performance, fault monitoring, and remote access.

[Table 3 on page 3](#) lists the device and network management features on the QFX Series, OCX Series, and EX4600.

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600

Feature	Typical Uses	Documentation
AI-Scripts and Advanced Insight Manager (AIM)—Automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems, and submit problem reports to Juniper Support Systems.	Fault management	Advanced Insight Scripts (AI-Scripts) Release Notes
Alarms and LEDs on the switch—Show status of hardware components and indicate warning or error conditions.	Fault management	Chassis Alarm Messages on a QFX3500 Device
Firewall filters—Control the packets that are sent to and from the network, balance network traffic, and optimize performance.	Performance management	<ul style="list-style-type: none">• Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices• Overview of Firewall Filters

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 (*continued*)

Feature	Typical Uses	Documentation
In-band management—Enables connection to the switch using the same interfaces through which customer traffic flows. Communication between the switch and a remote console is typically enabled using SSH and Telnet services. SSH provides secure encrypted communications, whereas Telnet provides unencrypted, and therefore less secure, access to the switch.	Remote access management	<ul style="list-style-type: none"> • Configuring SSH Service for Remote Access to the Router or Switch on page 96 • Configuring Telnet Service for Remote Access to a Router or Switch
Juniper Networks Junos OS automation scripts—Configuration and operations automation tools provided by Junos OS. These tools include commit scripts, operation scripts, event scripts, and event policies. Commit scripts enforce custom configuration rules, whereas operation scripts, event policies, and event scripts automate network troubleshooting and management.	<ul style="list-style-type: none"> • Configuration management • Performance management • Fault management 	<i>Junos OS Automation Library</i>
Junos OS command-line interface (CLI)—CLI configuration statements that enable you to configure the switch based on your networking requirements, such as security, service, and performance.	<ul style="list-style-type: none"> • Configuration management • Performance management • User access management • Remote access management 	<i>CLI User Guide</i>
Junos Space software—Multipurpose GUI-based network management system that includes a base platform, the Network Application Platform, and other optional applications such as Ethernet Design, Service Now, Service Insight, and Virtual Control. NOTE: Junos Space does not support the OCX Series.	<ul style="list-style-type: none"> • Configuration management • Performance management • Fault management 	<ul style="list-style-type: none"> • Understanding Junos Space Support on page 31 • Junos Space Network Application Platform User Guide
Junos XML API—XML representation of Junos OS configuration statements and operational mode commands. Junos XML configuration tag elements are the content to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device. The Junos XML API also includes tag elements that are the counterpart to Junos CLI configuration statements.	<ul style="list-style-type: none"> • Configuration management • Performance management • Fault management 	<ul style="list-style-type: none"> • Junos XML API Configuration Developer Reference • Junos XML API Operational Developer Reference

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 (*continued*)

Feature	Typical Uses	Documentation
NETCONF XML management protocol—XML-based management protocol that client applications use to request and change configuration information on routing, switching, and security platforms running Junos OS. The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as show , set , and commit to perform those operations.	<ul style="list-style-type: none"> • Configuration management • Performance management • Fault management 	<i>NETCONF XML Management Protocol Developer Guide</i>
<p>Operational mode commands—May be used to do the following:</p> <ul style="list-style-type: none"> • Monitor switch performance. For example, the show chassis routing-engine command shows the CPU utilization of the Routing Engine. High CPU utilization of the Routing Engine can affect performance of the switch. • View current activity and status of the device or network. For example, you can use the ping command to monitor and diagnose connectivity problems, and the traceroute command to locate points of failure on the network. 	<ul style="list-style-type: none"> • Performance management • Fault management 	CLI Explorer
Out-of-band management—Enables connection to the switch through a management interface. Out-of-band management is supported on two dedicated management Ethernet interfaces as well as on the console and auxiliary ports. The management Ethernet interfaces connect directly to the Routing Engine. No transit traffic is allowed through the interfaces, separating customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the switch.	Remote access management	<ul style="list-style-type: none"> • Connecting a QFX3500 Device to a Network for Out-of-Band Management • Connecting a QFX Series Device to a Management Console • Configuring Console and Auxiliary Port Properties on page 95

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 (continued)

Feature	Typical Uses	Documentation
SNMP Configuration Management MIB—Provides notification for configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.	Configuration management	<i>SNMP MIBs and Traps Reference</i>
SNMP MIBs and traps—Enable the monitoring of network devices from a central location. Use SNMP requests such as get and walk to monitor and view system activity. The QFX3500 switch supports SNMP Version 1 (v1), v2, and v3, and both standard and Juniper Networks enterprise-specific MIBs and traps.	Fault management	<ul style="list-style-type: none"> • <i>SNMP MIBs and Traps Reference</i> • Understanding the Implementation of SNMP on page 39
System log messages—Log details of system and user events, including errors. You can specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	<ul style="list-style-type: none"> • Fault management • User access management 	<ul style="list-style-type: none"> • <i>Junos OS System Log Messages Reference</i> • Overview of Junos OS System Log Messages on page 89 • Overview of Single-Chassis System Logging Configuration on page 89

Understanding Network Management Implementation on the QFabric System

This topic describes network management features on the QFabric system that are implemented differently than on other devices running Junos OS.

The following network management features are supported on the QFabric system:

- **System log messages**—The QFabric system monitors events that occur on its component devices, distributes system log messages about those events to all external system log message servers (hosts) that are configured, and archives the messages. Component devices include Node devices, Interconnect devices, Director devices, and the Virtual Chassis. You configure system log messages at the **[edit system syslog]** hierarchy level. Use the **show log filename** operational mode command to view messages.
- **Simple Network Management Protocol (SNMP) Version 1 (v1) and v2c**—SNMP monitors network devices from a central location. The SNMP implementation on the QFabric system supports the basic SNMP architecture of Junos OS with some limitations, including a reduced set of MIB objects, read-only access for SNMP communities, and limited support for SNMP requests. You configure SNMP at the **[edit snmp]** hierarchy level. Only the **show snmp statistics** operational mode command is supported, but you can issue SNMP requests using external SNMP client applications.

- **Advanced Insight Solutions (AIS)**—AIS provides tools and processes to automate the delivery of support services for the QFabric system. AIS components include Advanced Insight Scripts (AI-Scripts) and Advanced Insight Manager (AIM). You install AI-Scripts using the **request system scripts add** operational mode command. However, the **jais-activate-scripts.slax** file used during installation is preconfigured for the QFabric system and cannot be changed.



NOTE: Do not install Junos Space and AIS on the control plane network EX4200 switches or EX4200 Virtual Chassis in a QFX3000 QFabric system

Related Documentation

- [Advanced Insight Scripts \(AI-Scripts\) Release Notes](#)
- [Understanding Device and Network Management Features on page 3](#)
- [Overview of Junos OS System Log Messages on page 89](#)
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
- [SNMP MIBs Support on page 56](#)

Understanding Telnet on the QFabric System

This topic describes the support for the Telnet protocol on QFabric systems.

Telnet service is available for devices running Junos OS, including QFX Series devices. However, on QFabric systems, Telnet support is limited and the following conditions apply:

- You can telnet from a QFabric system to external devices that are connected to the QFabric system by way of the network Node group. To connect to these external devices, issue the **telnet** command from the QFabric default partition CLI.
- You cannot use the Telnet protocol to connect from the QFabric system default partition CLI to individual components. To access system components, you must issue the **request component login** command instead.

Related Documentation

- [request component login](#)
- [telnet](#)

Understanding Tracing and Logging Operations

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

The Junos OS supports remote tracing for the following processes:

- **chassisd**—Chassis-control process
- **eventd**—Event-processing process
- **cosd**—Class-of-service process

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



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

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

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

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



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

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

- **SNMP agent activity tracing operations**—Define tracing of the activities of SNMP agents on the switch. You configure SNMP agent activity tracing operations at the **[edit snmp]** hierarchy level.
- **Global switching tracing operations**—Define tracing for all switching operations. You configure global switching tracing operations at the **[edit ethernet-switching-options]** hierarchy level of the configuration.
- **Protocol-specific tracing operations**—Define tracing for a specific routing protocol. You configure protocol-specific tracing operations in the **[edit protocols]** hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global **traceoptions** statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.

- Tracing operations within individual routing protocol entities—Some protocols allow you to define more granular tracing operations. For example, in Border Gateway Protocol (BGP), you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.
- Interface tracing operations—Define tracing for individual interfaces and for the interface process itself. You define interface tracing operations at the **[edit interfaces]** hierarchy level of the configuration.
- Remote tracing—To enable system-wide remote tracing, configure the **destination-override syslog host** statement at the **[edit system tracing]** hierarchy level. This specifies the remote host running the system log process (syslogd), which collects the traces. Traces are written to files on the remote host in accordance with the syslogd configuration in **/etc/syslog.conf**. By default, remote tracing is not configured.

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

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



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

Related Documentation

- [Overview of Junos OS System Log Messages on page 89](#)

CHAPTER 2

Automation Scripts

- [Understanding Automation Scripts Support on page 11](#)
- [How Commit Scripts Work on page 12](#)
- [Avoiding Potential Conflicts When Using Multiple Commit Scripts on page 17](#)
- [Overview of Generating Persistent or Transient Configuration Changes on page 18](#)
- [Required Boilerplate for Commit Scripts on page 23](#)
- [How Op Scripts Work on page 24](#)
- [Required Boilerplate for Op Scripts on page 25](#)

Understanding Automation Scripts Support

This document describes the support for the Junos OS automation scripts on the QFabric system Director devices.

Junos OS automation consists of a suite of tools used to automate operational and configuration tasks on network devices running Junos OS. The automation tools, which leverage the native XML capabilities of the Junos OS, include commit scripts, operation (op) scripts, event policies and event scripts, and macros.



NOTE: Event policies and event scripts are not supported on the QFabric system at this time.

The QFabric system supports Junos OS automation scripts that are written in Stylesheet Language Alternative Syntax (SLAX) version 1.0.

Commit scripts automate the commit process and enforce custom configuration rules. You can use commit scripts to generate specific errors and warnings, and customize configurations and configuration templates. When a candidate configuration is committed, it is inspected by each active commit script. If a configuration violates your custom rules and the scripts generate an error, the commit fails. If the commit is successful, any configuration changes (both transient and permanent) are incorporated into the active configuration before it is passed to the Director software, which distributes the configuration to all applicable QFabric system components, including Node devices and Node servers.

Op scripts automate operational and troubleshooting tasks. Op scripts can be executed manually from the Junos OS CLI or NETCONF XML management protocol, or they can be called from another script.

The QFabric system supports the following automation script features:

- Commit scripts and op scripts are supported.
- Scripts written in SLAX version 1 are supported.
- Scripts are configured and deployed from the Director group. Since there is more than one Director device in a Director group, scripts must be deployed by each Director device or deployed in the shared media space.
- Scripts are stored in the shared media at this location:
`/pbdata/mgd_shared/partition-ip/var/db/scripts`. Under this directory, commit scripts are stored in the **commit** subdirectory, and op scripts are stored in the **op** subdirectory.
- Scripts are not stored in flash memory.

**Related
Documentation**

- [How Commit Scripts Work on page 12](#)
- [How Op Scripts Work on page 24](#)
- [Required Boilerplate for Commit Scripts on page 23](#)
- [Required Boilerplate for Op Scripts on page 25](#)
- [Controlling the Execution of Commit Scripts on page 99](#)

How Commit Scripts Work

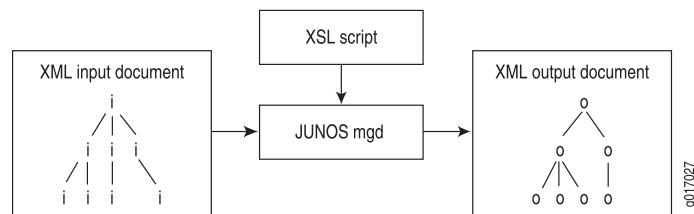
You enable commit scripts by listing the names of one or more commit script files at the **[edit system scripts commit]** hierarchy level. These scripts contain instructions that enforce custom configuration rules. Commit scripts are invoked during the commit process before the standard Junos OS validity checks are performed.

When you perform a commit operation, Junos OS executes each script in turn, passing the information in the candidate configuration to the scripts. The script inspects the configuration, performs the necessary tests and validations, and generates a set of instructions for performing certain actions. These actions include generating error, warning, and system log messages. If errors are generated, the commit operation fails and the candidate configuration remains unchanged. This is the same behavior that occurs with standard commit errors.

Commit scripts can also generate changes to the system configuration. Because the changes are loaded before the standard validation checks are performed, they are validated for correct syntax, just like statements already present in the configuration before the script is applied. If the syntax is correct, the configuration is activated and becomes the active, operational device configuration.

[Figure 1 on page 13](#) shows the flow of commit script input and output.

Figure 1: Commit Script Input and Output



Commit scripts cannot make configuration changes to protected statements or within protected hierarchies. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made. Failure to modify a protected configuration element does not halt the commit script or the commit process.

The following sections discuss several important concepts related to the commit script input and output:

- [Commit Script Input on page 13](#)
- [Commit Script Output on page 14](#)
- [Commit Scripts and the Junos OS Commit Model on page 15](#)

Commit Script Input

The input for a commit script is the postinheritance candidate configuration in Junos XML API format. The term *postinheritance* means that all configuration group values have been inherited by their targets in the candidate configuration and the inactive portions of the configuration have been removed. For more information about configuration groups, see the *CLI User Guide*.

When you issue the **commit** command, Junos OS automatically generates the candidate configuration in XML format and reads it into the management (mgd) process, at which time the input is evaluated by any commit scripts.

To display the XML format of the postinheritance configuration, issue the **show | display commit-scripts view** command:

```
[edit]
user@host# show | display commit-scripts view
```

To display all configuration groups data, including script-generated changes to the groups, issue the **show groups | display commit-scripts** command:

```
[edit]
user@host# show groups | display commit-scripts
```

To save the commit script input to a file, add the **save** command to the command line:

```
[edit]
user@host# show | display commit-scripts view | save filename.xml
```

By default, the file is placed in your home directory on the switch, router, or security device.

Commit Script Output

To specify the desired commit script output—including warning, error, and system log messages, persistent changes, and transient changes—the script can contain tags that appear in any order, in any number. The tags for specifying output are as follows:

- **<xnm:warning>**—Generates a warning message
- **<xnm:error>**—Generates an error message.
- **<syslog><message>**—Generates a system log message.
- **<change>**—Generates a persistent change to the configuration.
- **<transient-change>**—Generates a transient change to the configuration.
- **<xsl:call-template name="jcs:emit-change">**
 <xsl:with-param name="content">—Generates a persistent change relative to the current context node as defined by an XPath expression.
- **<xsl:call-template name="jcs:emit-change">**
 <xsl:with-param name="tag" select="transient-change"/>
 <xsl:with-param name="content">—Generates a transient change relative to the current context node as defined by an XPath expression.
- **<xsl:call-template name="jcs:emit-change">**
 <xsl:with-param name="message">
 <xsl:text>—Generates a warning message in conjunction with a configuration change. You can use this set of tags to generate a notification that the configuration has been changed.

Junos OS processes this output and performs the appropriate actions. Errors and warnings are passed back to the Junos OS CLI or to a Junos XML protocol client application. The presence of an error automatically causes the commit operation to fail. Persistent and transient changes are loaded into the appropriate configuration database.

To test the output of error, warning, and system log messages from commit scripts, issue the **commit check | display xml** command:

```
[edit]
user@host# commit check | display xml
```

To display a detailed trace of commit script processing, issue the **commit check | display detail** command:

```
[edit]
user@host# commit check | display detail
```



NOTE: System log messages do not appear in the trace output, so you cannot use the commit check operation to test script-generated system log messages. Furthermore, system log messages are written to the system log during a commit operation, but not during a commit check operation.

- Related Documentation**
- *Example: Protecting the Junos OS Configuration from Modification or Deletion.*
 - *jcs:emit-change Template*

Commit Scripts and the Junos OS Commit Model

Junos OS uses a commit model to update the device's configuration. This model allows you to make a series of changes to a candidate configuration without affecting the operation of the device. When the changes are complete, you can commit the configuration. The commit operation saves the candidate configuration changes into the current configuration.

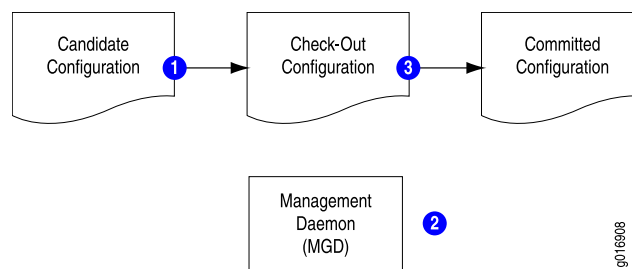
When you commit a set of changes in the candidate configuration, two methods are used to forward these changes to the current configuration:

- Standard commit model—Used when no commit scripts are active on the device.
- Commit script model—Incorporates commit scripts into the commit model.

Standard Commit Model

In the standard commit model, the management (mgd) process validates the candidate configuration based on standard Junos validation rules. If the configuration file is valid, it becomes the current active configuration. [Figure 2 on page 15](#) and the accompanying discussion explain how the standard commit model works:

Figure 2: Standard Commit Model



In the standard commit model, the software performs the following steps:

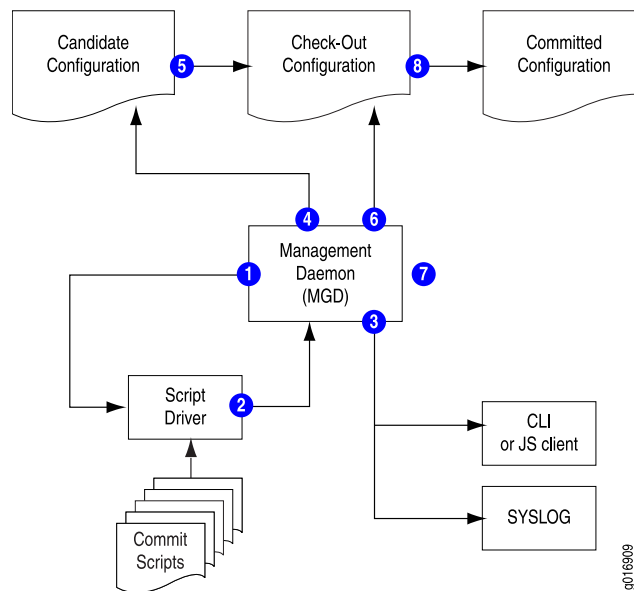
1. When the candidate configuration is committed, it is copied to become the checkout configuration.
2. The mgd process validates the checkout configuration.
3. If no error occurs, the checkout configuration is copied as the current active configuration.

Commit Model with Commit Scripts

When commit scripts are added to the standard commit model, the process becomes more complex. The mgd process first passes an XML-formatted checkout configuration to a script driver, which handles the verification of the checkout configuration by the commit scripts. When verification is complete, the script driver returns an XML *action file*

to the mgd process. The mgd process follows the instructions in the action file to update the candidate and checkout configurations, issue messages to the CLI, and write information to the system log as required. After processing the action file, the mgd process performs the standard Junos OS validation. [Figure 3 on page 16](#) and the accompanying discussion explain this process.

Figure 3: Commit Model with Commit Scripts Added



In the commit script model, Junos OS performs the following steps:

1. When the candidate configuration is committed, the mgd process sends the XML-formatted candidate configuration to the script driver.
2. Each enabled commit script is invoked against the candidate configuration, and each script can generate a set of actions for the mgd process to perform. The actions are collected in an XML action file.
3. The mgd process performs the following actions in response to **<error>**, **<warning>**, and **<syslog>** tag elements in the action file:
 - **<error>**—The mgd process halts the commit process (that is, the commit operation fails), returns an error message to the CLI or Junos XML protocol client, and takes no further action.
 - **<warning>**—The mgd process forwards the message to the CLI or the Junos XML protocol client.
 - **<syslog>**—The mgd process forwards the message to the system log process.
4. If the action file includes any **<change>** tag elements, the mgd process loads the requested changes into the candidate configuration.
5. The candidate configuration is copied to become the checkout configuration.
6. If the action file includes any **<transient-change>** tag elements, the mgd process loads the requested changes into the checkout configuration.

7. The mgd process validates the checkout configuration.
8. If there are no validation errors, the checkout configuration is copied to become the current active configuration.



NOTE: Commit scripts cannot make configuration changes to protected statements or within protected hierarchies. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made. Failure to modify a protected configuration element does not halt the commit script or the commit process.

Changes that are made to the candidate configuration during the commit operation are not evaluated by the custom rules during that commit operation. However, persistent changes are maintained in the candidate configuration and are evaluated by the custom rules during subsequent commit operations. For more information about how commit scripts change the candidate configuration, see [“Avoiding Potential Conflicts When Using Multiple Commit Scripts” on page 17](#).

Transient changes are never evaluated by the custom rules in commit scripts, because they are made to the checkout configuration only after the commit scripts have evaluated the candidate configuration and the candidate is copied to become the checkout configuration. To remove a transient change from the configuration, remove, disable, or deactivate the commit script (as discussed in *Controlling Execution of Commit Scripts During Commit Operations*), or comment out the code that generates the transient change.

For more information about differences between persistent and transient changes, see [“Overview of Generating Persistent or Transient Configuration Changes” on page 18](#).

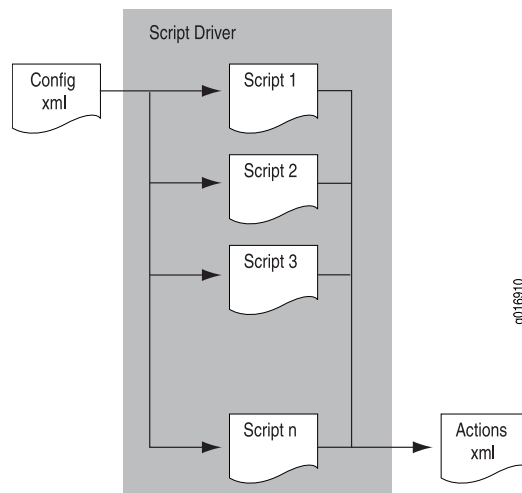
**Related
Documentation**

- [Avoiding Potential Conflicts When Using Multiple Commit Scripts on page 17](#)

Avoiding Potential Conflicts When Using Multiple Commit Scripts

When you use multiple commit scripts, each script evaluates the original candidate configuration file. Changes made by one script are not evaluated by the other scripts. This means that conflicts between scripts might not be resolved when the scripts are first applied to the configuration. The commit scripts are executed in the order they are listed at the **[edit system scripts commit]** hierarchy level, as illustrated in [Figure 4 on page 18](#).

Figure 4: Configuration Evaluation by Multiple Commit Scripts



As an example of a conflict between commit scripts, suppose that commit script **A.xsl** is created to ensure that the device uses the domain name server with IP address 192.168.0.255. Later, the DNS server's address is changed to 192.168.255.255 and a second script, **B.xsl**, is added to check that the device uses the DNS server with that address. However, script **A.xsl** is not removed or disabled.

Because each commit script evaluates the original candidate configuration, the final result of executing both scripts **A.xsl** and **B.xsl** depends on which DNS server address is configured in the original candidate configuration. If the now outdated address of 192.168.0.255 is configured, script **B.xsl** changes it to 192.168.255.255. However, if the correct address of 192.168.255.255 is configured, script **A.xsl** changes it to the incorrect value 192.168.0.255.

As another example of a potential conflict between commit scripts, suppose that a commit script protects a hierarchy using the **protect** attribute. If a second commit script attempts to modify or delete the hierarchy or the statements within the hierarchy, Junos OS issues a warning during the commit process and prevents the configuration change.

Exercise care to ensure that you do not introduce conflicts between scripts like those described in the examples. As a method of checking for conflicts with persistent changes, you can issue two separate **commit** commands.

Related Documentation

- [How Commit Scripts Work on page 12](#)

Overview of Generating Persistent or Transient Configuration Changes

Junos OS commit scripts enforce custom configuration rules. When a candidate configuration includes statements that you have decided must not be included in your configuration, or when the candidate configuration omits statements that you have

decided are required, commit scripts can automatically change the configuration and thereby correct the problem.

- [Differences Between Persistent and Transient Changes on page 19](#)
- [Interaction of Configuration Changes and Configuration Groups on page 22](#)
- [Tag Elements and Templates for Generating Changes on page 22](#)

Differences Between Persistent and Transient Changes

Configuration changes made by commit scripts can be *persistent* or *transient*.

A persistent change remains in the candidate configuration and affects routing operations until you explicitly delete it, even if you subsequently remove or disable the commit script that generated the change and reissue the **commit** command. In other words, removing the commit script does not cause a persistent change to be removed from the configuration.

A transient change, in contrast, is made in the *checkout configuration* but not in the candidate configuration. The checkout configuration is the configuration database that is inspected for standard Junos OS syntax just before it is copied to become the active configuration on the device. If you subsequently remove or disable the commit script that made the change and reissue the **commit** command, the change is no longer made to the checkout configuration and so does not affect the active configuration. In other words, removing the commit script effectively removes a transient change from the configuration.

A common use for transient changes is to eliminate the need to repeatedly configure and display well-known policies, thus allowing these policies to be enforced implicitly. For example, if MPLS must be enabled on every interface with an International Organization for Standardization (ISO) protocol enabled, the change can be transient, so that the repetitive or redundant configuration data need not be carried or displayed in the candidate configuration. Furthermore, transient changes allow you to write script instructions that apply the change only if a set of conditions is met.

Persistent and transient changes are loaded into the configuration in the same manner that the **load replace** configuration mode command loads an incoming configuration. When generating a persistent or transient change, adding the **replace="replace"** attribute to a configuration element produces the same behavior as a **replace:** tag in a **load replace** operation.

By default, Junos OS merges the incoming configuration and the candidate configuration. New statements and hierarchies are added, and conflicting statements are overridden. When generating a persistent or transient change, if you add the **replace="replace"** attribute to a configuration element, Junos OS replaces the existing configuration element with the incoming configuration element. If the **replace="replace"** attribute is added to a configuration element, but there is no existing element of the same name in the current configuration, the incoming configuration element is added into the configuration. Elements that do not have the **replace** attribute are merged into the configuration.

Persistent and transient changes are loaded before the standard Junos validation checks are performed. This means any configuration changes introduced by a commit script are

validated for correct syntax. If the syntax is correct, the new configuration becomes the active, operational device configuration.

Protected elements in the configuration hierarchy cannot be modified or deleted by either a persistent or a transient change. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made, and proceeds with the commit.

Persistent and transient changes have several important differences, as described in [Table 4 on page 20](#).

Table 4: Differences Between Persistent and Transient Changes

Persistent Changes	Transient Changes
<p>A persistent change is represented in a commit script by the <change> tag.</p> <p>Another way to represent a persistent change is with the content parameter inside a call to the jcs:emit-change template.</p> <p>The jcs:emit-change template is a helper template contained in the junos.xsl import file.</p>	<p>A transient change is represented in a commit script by the <transient-change> tag.</p> <p>Another way to represent a transient change is to use the content parameter and the tag transient parameter inside a call to the jcs:emit-change template.</p>
<p>You can use persistent changes to perform any Junos XML protocol operation, such as activate, deactivate, delete, insert (reorder), comment (annotate), and replace sections of the configuration.</p>	<p>Like persistent changes, you can use transient changes to perform any Junos XML protocol operation. However, some Junos XML protocol operations do not make sense to use with transient changes, such as generating comments and inactive settings.</p>
<p>Persistent changes are always loaded during the commit process if no errors are generated by any commit scripts or by the standard Junos OS validity check.</p>	<p>For transient changes to be loaded, you must include the allow-transients statement at the [edit system scripts commit] hierarchy level. If you enable a commit script that generates transient changes and you do not include the allow-transients statement in the configuration, the CLI generates an error message and the commit operation fails.</p> <p>Like persistent changes, transient changes must pass the standard Junos OS validity check.</p> <p>You cannot use a commit script to generate the allow-transients statement at the [edit system scripts commit] hierarchy level. Rather, you must include this statement directly by using the CLI.</p>

Table 4: Differences Between Persistent and Transient Changes (*continued*)

Persistent Changes	Transient Changes
<p>Persistent changes work like the load replace configuration mode command, and the change is added to the candidate configuration.</p> <p>When generating a persistent change, if you add the replace="replace" attribute to a configuration element, Junos OS replaces the existing element in the candidate configuration with the incoming configuration element. If there is no existing element of the same name in the candidate configuration, the incoming configuration element is added into the configuration. Elements that do not have the replace attribute are merged into the configuration.</p>	<p>Transient changes work like the load replace configuration mode command, and the change is added to the checkout configuration.</p> <p>When generating a transient change, if you add the replace="replace" attribute to a configuration element, Junos OS replaces the existing element in the checkout configuration with the incoming configuration element. If there is no existing element of the same name in the checkout configuration, the incoming configuration element is added into the configuration. Elements that do not have the replace attribute are merged into the configuration.</p> <p>Transient changes are not copied to the candidate configuration. For this reason, transient changes are not saved in the configuration if the associated commit script is deleted or deactivated.</p>
<p>After a persistent change is committed, the software treats it like a change you make by directly editing and committing the candidate configuration.</p> <p>After the persistent changes are copied to the candidate configuration, they are copied to the checkout configuration. If the changes pass the standard Junos OS validity checks, the changes are propagated to the switch, router, or security device components.</p>	<p>Each time a transient change is committed, the software updates the checkout configuration database. After the transient changes pass the standard Junos OS validity checks, the changes are propagated to the device components.</p>
<p>After committing a script that causes a persistent change to be generated, you can view the persistent change by issuing the show configuration mode command:</p> <pre>user@host# show</pre> <p>This command displays persistent changes only, not transient changes.</p>	<p>After committing a script that causes a transient change to be generated, you can view the transient change by issuing the show display commit-scripts configuration mode command:</p> <pre>user@host# show display commit-scripts</pre> <p>This command displays both persistent and transient changes.</p>
<p>Persistent changes must conform to your custom configuration design rules as dictated by commit scripts.</p> <p>This does not become apparent until after a second commit operation because persistent changes are not evaluated by commit script rules on the current commit operation. The subsequent commit operation fails if the persistent changes do not conform to the rules imposed by the commit scripts configured during the first commit operation.</p>	<p>Transient changes are never tested by and do not need to conform to your custom rules. This is caused by the order of operations in the Junos OS commit model, which is explained in detail in “Commit Scripts and the Junos OS Commit Model” on page 15.</p>
<p>A persistent change remains in the configuration even if you delete, disable, or deactivate the commit script instructions that generated the change.</p>	<p>If you delete, disable, or deactivate the commit script instructions that generate a transient change, the change is removed from the configuration after the next commit operation. In short, if the associated instructions or the entire commit script is removed, the transient change is also removed.</p>

Table 4: Differences Between Persistent and Transient Changes (*continued*)

Persistent Changes	Transient Changes
As with direct CLI configuration, you can remove a persistent change by rolling back to a previous configuration that did not include the change and issuing the commit command. However, if you do not disable or deactivate the associated commit script, and the problem that originally caused the change to be generated still exists, the change is automatically regenerated when you issue another commit command.	You cannot remove a transient change by rolling back to a previous configuration.
You can alter persistent changes directly by editing the configuration using the CLI.	<p>You cannot directly alter or delete a transient change by using the Junos OS CLI, because the change is not in the candidate configuration.</p> <p>To alter the contents of a transient change, you must alter the statements in the commit script that generates the transient change.</p>

Interaction of Configuration Changes and Configuration Groups

Any configuration change you can make by directly editing the configuration using the Junos OS command-line interface (CLI) can also be generated by a commit script as a persistent or transient change. This includes values specified at a specific hierarchy level or in configuration groups. As with direct CLI configuration, values specified in the *target* override values inherited from a configuration group. The target is the statement to which you apply a configuration group by including the **apply-groups** statement.

If you define persistent or transient changes as belonging to a configuration group, the configuration groups are applied in the order you specify in the **apply-groups** statements, which you can include at any hierarchy level except the top level. You can also disable inheritance of a configuration group by including the **apply-groups-except** statement at any hierarchy level except the top level.



CAUTION: Each commit script inspects the postinheritance view of the configuration. If a candidate configuration contains a configuration group, be careful when using a commit script to change the related target configuration, because doing so might alter the intended inheritance from the configuration group.

Also be careful when using a commit script to change a configuration group, because the configuration group might be generated by an application that performs a load replace operation on the group during each commit operation.

For more information about configuration groups, see the *CLI User Guide*.

Tag Elements and Templates for Generating Changes

To generate changes, you can use the **jcs:emit-change** template, which implicitly includes **<change>** and **<transient-change>** XML elements; or you can explicitly include **<change>**

and `<transient-change>` XML elements. Using the `jcs:emit-change` template allows you to set the hierarchical context of the change once rather than multiple times.

The `<change>` and `<transient-change>` elements are similar to the `<load-configuration>` operation defined by the Junos XML management protocol. The possible contents of the `<change>` and `<transient-change>` elements are the same as the contents of the `<configuration>` tag element used in the Junos XML protocol operation `<load-configuration>`. For complete details about the `<load-configuration>` element, see the *Junos XML Management Protocol Developer Guide*.

Required Boilerplate for Commit Scripts

When you write commit scripts, you use Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) tools provided with Junos OS. These tools include basic boilerplate that you must include in all commit scripts, optional extension functions that accomplish scripting tasks more easily, and named templates that make commit scripts easier to read and write, which you import from a file called `junos.xsl`. For more information about the extension functions and templates, see *Junos Script Automation: Understanding Extension Functions in the jcs and slax Namespaces* and *Junos Script Automation: Named Templates in the jcs Namespace Overview*.

Commit scripts are based on Junos XML and Junos XML protocol tag elements. Like all XML elements, angle brackets enclose the name of a Junos XML or Junos XML protocol tag element in its opening and closing tags. This is an XML convention, and the brackets are a required part of the complete tag element name. They are not to be confused with the angle brackets used in the documentation to indicate optional parts of Junos OS CLI command strings.

You must include either XSLT or SLAX boilerplate as the starting point for all commit scripts that you create. The XSLT boilerplate follows:

XSLT Boilerplate for Commit Scripts

```

1  <?xml version="1.0" standalone="yes"?>
2  <xsl:stylesheet version="1.0"
3    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4    xmlns:junos="http://xml.juniper.net/junos/*/junos"
5    xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6    xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
7    <xsl:import href="../../../import/junos.xsl"/>

8    <xsl:template match="configuration">
9      <!-- ... Insert your code here ... -->
10   </xsl:template>
11 </xsl:stylesheet>
```

Line 1 is the Extensible Markup Language (XML) processing instruction (PI). This PI specifies that the code is written in XML using version 1.0. The XML PI, if present, must be the first noncomment token in the script file.

```
1  <?xml version="1.0"?>
```


Lines 2 through 6 set the style sheet element and the associated namespaces. Line 2 sets the style sheet version as 1.0. Lines 3 through 6 list all the namespace mappings commonly used in commit scripts. Not all of these prefixes are used in this example, but it is not an error to list namespace mappings that are not referenced. Listing all namespace mappings prevents errors if the mappings are used in later versions of the script.

```
2 <xsl:stylesheet version="1.0"
3   xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4   xmlns:junos="http://xml.juniper.net/junos/*/junos"
5   xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6   xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
```

Line 7 is an XSLT import statement. It loads the templates and variables from the file referenced as `../import/junos.xsl`, which ships as part of the Junos OS. The `junos.xsl` file contains a set of named templates you can call in your scripts. These named templates are discussed in *Junos Script Automation: Named Templates in the jcs Namespace Overview* and *Junos Named Templates in the jcs Namespace Summary*.

```
7 <xsl:import href="../import/junos.xsl"/>
```

Line 8 defines a template that matches the `<configuration>` element, which is the node selected by the `<xsl:template match="/">` template, contained in the `junos.xsl` import file. The `<xsl:template match="configuration">` element allows you to exclude the `/configuration/` root element from all XML Path Language (XPath) expressions in the script and begin XPath expressions with the top Junos OS hierarchy level. For more information, see *XPath Overview*.

```
8 <xsl:template match="configuration">
```

Add your code between Lines 8 and 9.

Line 9 closes the template.

```
9 </xsl:template>
```

Line 10 closes the style sheet and the commit script.

```
10 </xsl:stylesheet>
```

SLAX Boilerplate for Commit Scripts

The corresponding SLAX boilerplate is as follows:

```
version 1.0;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";

match configuration {
/*
* Insert your code here
*/
}
```

How Op Scripts Work

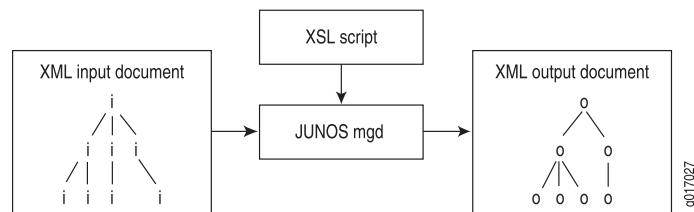
Op scripts execute Junos OS operational commands and inspect the resulting output. After inspection, op scripts can automatically correct errors within the device running Junos OS based on this output.

You add op scripts to device operations by listing the filenames of one or more op script files within the **[edit system scripts op]** hierarchy level. These files must be added to the appropriate op script file directory. For more information about op script file directories, see *Storing Scripts in Flash Memory*. Once added to the device, op scripts are invoked from the command line, using the **op filename** command.

You can use op scripts to generate changes to the device configuration by including the **<load-configuration>** tag element. Because the changes are loaded before the standard validation checks are performed, they are validated for correct syntax, just like statements already present in the configuration before the script is applied. If the syntax is correct, the configuration is activated and becomes the active, operational device configuration.

Figure 5 on page 25 shows a high-level view of the flow of op script input and output.

Figure 5: Op Script Input and Output



Required Boilerplate for Op Scripts

When you write operation (op) scripts, you use Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) tools provided with Junos OS. These tools include basic boilerplate that you must include in all op scripts, optional extension functions that accomplish scripting tasks more easily, and named templates that make scripts easier to read and write, which you import from a file called **junos.xsl**. For more information about the extension functions and templates, see *Junos Script Automation: Understanding Extension Functions in the jcs and slax Namespaces* and *Junos Script Automation: Named Templates in the jcs Namespace Overview*.

Op scripts are based on Junos XML and Junos XML protocol tag elements. Like all XML elements, angle brackets enclose the name of a Junos XML or Junos XML protocol tag element in its opening and closing tags. This is an XML convention, and the brackets are a required part of the complete tag element name. They are not to be confused with the angle brackets used in the documentation to indicate optional parts of Junos OS CLI command strings.

You must include either XSLT or SLAX boilerplate as the starting point for all op scripts that you create. The XSLT boilerplate follows:

XSLT Boilerplate for Op Scripts

```

1 <?xml version="1.0" standalone="yes"?>
2 <xsl:stylesheet version="1.0"
3   xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4   xmlns:junos="http://xml.juniper.net/junos/*/junos"
5   xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6   xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
7   <xsl:import href="../import/junos.xsl"/>

```



```
8  <xsl:template match="/">
9    <op-script-results>
10     <!-- ... insert your code here ... -->
11   </op-script-results>
12 </xsl:template>
   <!-- ... insert additional template definitions here ... -->
12 </xsl:stylesheet>
```

Line 1 is the Extensible Markup Language (XML) processing instruction (PI), which marks this file as XML and specifies the version of XML as 1.0. The XML PI, if present, must be the first non-comment token in the script file.

```
1  <?xml version="1.0"?>
```

Line 2 opens the style sheet and specifies the XSLT version as 1.0.

```
2  <xsl:stylesheet version="1.0"
```

Lines 3 through 6 list all the namespace mappings commonly used in operation scripts. Not all of these prefixes are used in this example, but it is not an error to list namespace mappings that are not referenced. Listing all namespace mappings prevents errors if the mappings are used in later versions of the script.

```
3  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4  xmlns:junos="http://xml.juniper.net/junos/*/junos"
5  xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6  xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
```

Line 7 is an XSLT import statement. It loads the templates and variables from the file referenced as `../import/junos.xsl`, which ships as part of Junos OS (in the file `/usr/libdata/cscript/import/junos.xsl`). The `junos.xsl` file contains a set of named templates you can call in your scripts. These named templates are discussed in *Junos Script Automation: Named Templates in the jcs Namespace Overview* and *Junos Named Templates in the jcs Namespace Summary*.

```
7  <xsl:import href="../import/junos.xsl"/>
```

Line 8 defines a template that matches the `</>` element. The `<xsl:template match="/">` element is the root element and represents the top level of the XML hierarchy. All XML Path Language (XPath) expressions in the script must start at the top level. This allows the script to access all possible Junos XML and Junos XML protocol remote procedure calls (RPCs). For more information, see *XPath Overview*.

```
8  <xsl:template match="/">
```

After the `<xsl:template match="/">` tag element, the `<op-script-results>` and `</op-script-results>` container tags must be the top-level child tags, as shown in Lines 9 and 10.

```
9    <op-script-results>
10     <!-- ... insert your code here ... -->
11   </op-script-results>
```

Line 11 closes the template.

```
11  </xsl:template>
```

Between Line 11 and Line 12, you can define additional XSLT templates that are called from within the `<xsl:template match="/">` template.

Line 12 closes the style sheet and the op script.

```
12 </xsl:stylesheet>
```

SLAX Boilerplate for Op Scripts

The corresponding SLAX boilerplate is as follows:

```
version 1.0;
```

```
ns junos = "http://xml.juniper.net/junos/*/junos";  
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";  
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";  
import "../import/junos.xsl";
```

```
match / {  
  <op-script-results> {  
    /*  
      * Insert your code here  
    */  
  }  
}
```


CHAPTER 3

Fabric OAM

- [Overview of Internal Fabric Monitoring on page 29](#)

Overview of Internal Fabric Monitoring

Internal fabric monitoring is a feature of the Operation, Administration, and Maintenance (OAM) of the QFabric system. This feature enables you to validate the flow path of protocol data units (PDUs) across a given VLAN on the QFabric system using the unicast ping, multicast ping, and traceroute operations.

Internal fabric monitoring is useful for fault detection on the QFabric system. For example, if a PDU reaches a destination that is not part of the VLAN configuration, the operation (unicast ping, multicast ping, or traceroute) displays the exception on the console at runtime.

The unicast and multicast ping operations send PDUs from a source interface (called the source fabric maintenance endpoint [FMEP]) to a destination FMEP. The destination FMEP sends a response to the source FMEP when the PDUs are received.

The traceroute operation, also called a flow linktrace, traces the path taken by a specific, learned unicast flow from a source FMEP to a destination FMEP in a VLAN. The source and destination FMEPs may be on the same Node device, different Node devices connected to the same Interconnect device, or different Node devices connected to different Interconnect devices. The flow path is the sequence of Packet Forwarding Engine forwarding hops along which the PDU travels. The hop-by-hop sequence and number of hops are reported in terms of fabric maintenance intermediate points (FMIPs), which are interfaces on the Packet Forwarding Engine of the Interconnect device. An FMIP sends a response to the source FMEP when the traceroute PDU is received.

The following internal fabric monitoring commands are supported:

- **show oam fabric flow specification**
- **show oam fabric interfaces**
- **ping fabric unicast-flow**
- **ping fabric multicast-flow**
- **traceroute fabric unicast-flow**

The following are the main components of the internal fabric monitoring feature:

- **FMEP**—Represents the source or destination point (endpoint) in the monitoring operations. An FMEP is an interface through which PDUs are sent (source FMEP) or received (destination FMEP). Upon receipt of the PDUs, the destination FMEP sends a response to the source FMEP to validate the monitoring flow. FMEPs are associated with a VLAN in the fabric maintenance association (FMA) configuration, and the source and destination FMEP addresses are configured in the flow specification.
- **FMA**—Associates a set of FMEPs with a VLAN. The FMA defines the VLAN and FMEP parameters, including the VLAN name, FMEP identifiers, FMEP names, and the interface names of the FMEPs. The FMEPs defined in the FMA are the source and destination FMEPs used in the monitoring commands.



NOTE: A default FMA is automatically created for each Node group in the QFabric system. The default FMA is used to send error response PDUs (for example, in the case of a VLAN leak) and responses to PDUs that are not mapped to a specific interface in the QFabric system.

- **Flow specification**—Configures the flow type and FMEP addressing parameters. Unicast flow types include an Ethernet type (other than IPv4) and Ethernet IPv4. Multicast flow types include the Ethernet IPv4 and VLAN flood type. The flow specification also defines parameters within each flow type, such as MAC or IPv4 addresses of the source and destination FMEPs. The names and identifiers of these FMEPs are configured in the FMA parameters.

To enable internal fabric monitoring, configure the **fabric-maintenance-associations** and **flow-specs** statements at the **[edit protocols oam fabric]** hierarchy level.

The **ping fabric unicast-flow**, **ping fabric multicast-flow**, and **traceroute fabric unicast-flow** commands require that you specify the flow specification and FMA names, as well as the source and destination FMEP names.

**Related
Documentation**

- [Configuring a Fabric Maintenance Association on page 103](#)
- [Configuring Flow Specifications on page 104](#)
- [fabric \(OAM\) on page 237](#)
- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

CHAPTER 4

Junos Space

- [Understanding Junos Space Support on page 31](#)
- [Preparing the Device for Junos Space Management on page 32](#)

Understanding Junos Space Support

The Juniper Networks Junos Space application, running on a JA1500 appliance or a Junos Space Virtual Appliance, is a comprehensive platform for building and deploying applications for collaboration, productivity, and network infrastructure and operations management. Junos Space provides a runtime environment implemented as a fabric of virtual and physical appliances.

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

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



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

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

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

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

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

For more information about Junos Space, go to:

http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html

**Related
Documentation**

- [Configuring SNMP on page 121](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 96](#)

Preparing the Device for Junos Space Management

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

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



.....

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

.....

To prepare the device before using Junos Space:

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

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

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

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

See “[Configuring SNMP](#)” on page 121.

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

See “[Configuring SSH Service for Remote Access to the Router or Switch](#)” on page 96.

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

http://www.juniper.net/techpubs/en_US/junos-space/3/platform/information-products/pathway/pages/junos-space-administration.pdf.html

.

**Related
Documentation**

- *Configuring a QFX3500 Device as a Standalone Switch*
- *QFabric System Initial and Default Configuration Information*
- *Performing the QFabric System Initial Setup on a QFX3100 Director Group*
- [Configuring SNMP on page 121](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 96](#)

CHAPTER 5

sFlow Technology

- [Overview of sFlow Technology on page 35](#)

Overview of sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS fully supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

sFlow technology implements the following two sampling mechanisms:

- **Packet-based sampling**—Samples one packet out of a specified number of packets from an interface enabled for sFlow technology. Only the first 128 bytes of each packet are sent to the collector. Data collected include the Ethernet, IP, and TCP headers, along with other application-level headers (if present). Although this type of sampling might not capture infrequent packet flows, the majority of flows are reported over time, allowing the collector to generate a reasonably accurate representation of network activity. You configure packet-based sampling when you specify a sample rate.
- **Time-based sampling**—Samples interface statistics (counters) at a specified interval from an interface enabled for sFlow technology. Statistics such as Ethernet interface errors are captured. You configure time-based sampling when you specify a polling interval.

An sFlow monitoring system consists of an sFlow agent embedded in the device and up to four external collectors. On a QFX Series standalone switch, the sFlow agent performs packet sampling and gathers interface statistics, and then combines the information into UDP datagrams that are sent to the sFlow collectors. An sFlow collector can be connected to the switch through the management network or data network. The software forwarding infrastructure daemon (SFID) on the switch looks up the next-hop address for the specified collector IP address to determine whether the collector is reachable by way of the management network or data network.



NOTE: On the QFX Series standalone switches, if you configure sFlow technology monitoring on multiple interfaces and a high sampling rate, we recommend that you specify a collector that is on the data network instead of the management network. Having a high volume of sFlow technology monitoring traffic on the management network might interfere with other management interface traffic.

On a QFabric system, the sFlow technology architecture is distributed. The global sFlow technology configuration defined on the QFabric system Director device is distributed to Node groups that have sFlow sampling configured on their interfaces. The sFlow agent has a separate sampling entity, known as a *subagent*, running on each Node device. Each subagent has its own independent state and forwards its own sample information (datagrams) directly to the sFlow collectors.

On the QFabric system, an sFlow collector must be reachable through the data network. Because each Node device has all routes stored in the default routing instance, the collector IP address should be included in the default routing instance to ensure the collector's reachability from the Node device.

Regardless of the rate of traffic or the configured sampling interval, a datagram is sent whenever its size reaches the maximum Ethernet transmission unit (MTU) of 1500 bytes, or whenever a 250-ms timer expires, whichever occurs first. The timer ensures that a collector receives regularly sampled data.

To ensure sampling accuracy and efficiency, QFX Series devices use adaptive sFlow sampling. Adaptive sampling monitors the overall incoming traffic rate on the device and provides feedback to the interfaces to dynamically adapt their sampling rate to traffic conditions. The sFlow agent reads the statistics on the interfaces every 5 seconds and identifies five interfaces with the highest number of samples. On a standalone switch, when the CPU processing limit is reached, a binary backoff algorithm is implemented to reduce the sampling load of the top five interfaces by half. The adapted sampling rate is then applied to other interfaces.

On a QFabric system, sFlow technology monitors the interfaces on each Node device as a group, and implements the binary backoff algorithm based on the traffic on that group of interfaces.

Using adaptive sampling prevents overloading of the CPU and keeps the device operating at its optimum level even when there is a change in traffic patterns on the interfaces. The reduced sampling rate is used until the device is rebooted or when a new sampling rate is configured.

The sFlow collector uses the IP address of the sFlow agent to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID for the sFlow agent remains constant. If you do not assign an IP address to the agent, an IP address will be assigned to the agent using the IP address of a configured interface.

On the QFX Series standalone switches, the following priority is used to determine which interface will be used:

1. Management Ethernet interface me0 IP address
2. Any Layer 3 interface if the me0 IP address is not available

If a particular interface is not configured, the IP address of the next interface in the priority list is used as the IP address for the agent. Once an IP address is assigned to the agent, the agent ID is not modified until the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent.

In addition, you can explicitly configure the IP address for the source data (sFlow datagrams). On the QFX Series standalone switches, if you do not configure that address, the following priority is used:

- Any Layer 3 interface IP address
- The me0 IP address if no Layer 3 interface IP address is available

On the QFabric system, the following default values are used if the optional parameters are not configured:

- Agent ID is the management IP address of the default partition.
- Source IP is the management IP address of the default partition.

In addition, the QFabric system subagent ID (which is included in the sFlow datagrams) is the ID of the Node group from which the datagram is sent to the collector.



NOTE: On QFX5100 standalone switches and the QFX Series Virtual Chassis (with QFX3500 and QFX3600 switches), egress firewall filters are not applied to sFlow sampling packets. On these platforms, the software architecture is different from that on other QFX Series devices, and sFlow packets are sent by the Routing Engine (not the line card on the host) and are not transiting the switch. Egress firewall filters affect data packets that are transiting a switch but do not affect packets sent by the Routing Engine. As a result, sFlow sampling packets are always sent to the sFlow collector.

On the QFX Series, limitations of sFlow traffic sampling include:

- sFlow sampling on ingress interfaces does not capture CPU-bound traffic.
- sFlow sampling on egress interfaces does not support broadcast and multicast packets.
- Egress samples do not contain modifications made to the packet in the egress pipeline.

- If a packet is discarded because of a firewall filter, the reason code for discarding the packet is not sent to the collector.
- The **out-priority** field for a VLAN is always set to 0 (zero) on ingress and egress samples.
- You cannot configure sFlow monitoring on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.

**Related
Documentation**

- [Example: Monitoring Network Traffic Using sFlow Technology on page 116](#)
- [Configuring sFlow Technology on page 115](#)

CHAPTER 6

SNMP

- [Understanding the Implementation of SNMP on page 39](#)
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
- [Fabric Chassis MIB on page 44](#)
- [Utility MIB on page 48](#)
- [SNMPv3 Overview on page 49](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50](#)
- [Understanding RMON on page 51](#)
- [RMON MIB Event, Alarm, Log, and History Control Tables on page 53](#)
- [Understanding Health Monitoring on page 55](#)
- [SNMP MIBs Support on page 56](#)
- [SNMP Traps Support on page 72](#)
- [MIB Objects for the QFX Series on page 85](#)

Understanding the Implementation of SNMP

The QFX Series products support the Simple Network Management Protocol (SNMP) that is implemented in the Junos OS software.



NOTE: By default, SNMP is not enabled on devices running Junos OS. For information on enabling SNMP on a device running Junos OS, see [“Configuring SNMP” on page 121](#).

A typical SNMP implementation includes the following components:

- **Network management system (NMS)**—The NMS is a combination of hardware and software that is used to monitor and administer a network. Software running on the NMS includes the SNMP manager, which collects information about network connectivity, activity, and events by polling the managed devices.
- **Managed device**—A managed device (also called a network element) is any device managed by the NMS. Routers and switches are common examples of managed devices. The SNMP agent is the SNMP process that resides on the managed device and communicates with the NMS.

- **SNMP agent**—The SNMP agent exchanges network management information with SNMP manager software running on an NMS, or host. The agent responds to requests for information and actions from the manager. The agent also controls access to the agent's MIB, the collection of objects that can be viewed or changed by the SNMP manager.

SNMP data is stored in a highly structured, hierarchical format known as a management information base (MIB). The MIB structure is based on a tree structure, which defines a grouping of objects into related sets. Each object in the MIB is associated with an object identifier (OID), which names the object. The “leaf” in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs in your network device. The SNMP implementation in Junos OS uses both standard (developed by IETF and documented in RFCs) and Juniper Networks enterprise-specific MIBs.

Communication between the agent and the manager occurs in one of the following forms:

- **Get, GetBulk, and GetNext** requests—The manager requests information from the agent; the agent returns the information in a **Get** response message.
- **Set** requests—The manager changes the value of a MIB object controlled by the agent; the agent indicates status in a **Set** response message.
- **Traps** notification—The agent sends traps to notify the manager of significant events that occur on the network device.

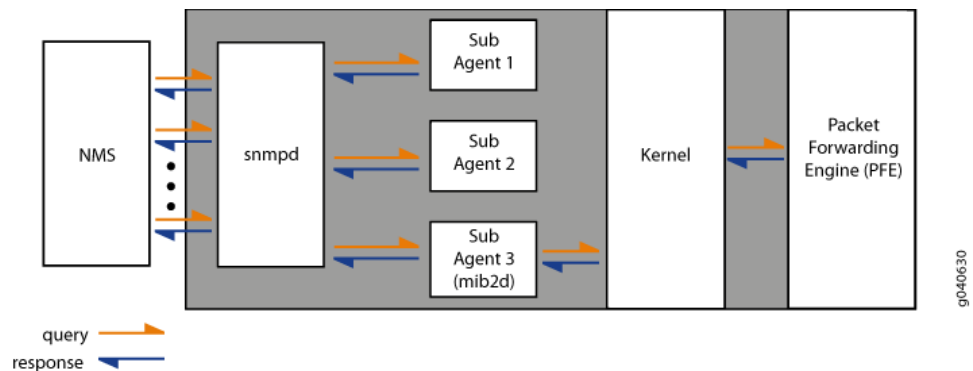
The processes maintaining the SNMP management data include:

- A master SNMP agent (known as SNMP process, or `snmpd`) that resides on the managed device and is managed by the NMS or host.
- Various subagents that reside on different modules of Junos OS, such as the Routing Engine, and are managed by the master SNMP agent.
- Junos OS processes that share data with the subagents when polled for SNMP data (for example, interface-related MIBs).

When an NMS polls the master agent for data, the master agent immediately shares the data with the NMS if the requested data is available from the master agent or one of the subagents. However, if the requested data is not maintained by the master agent or subagents, the subagent polls the Junos OS kernel or the process that maintains that data. The Junos OS kernel may need to get the data from the Packet Forwarding Engine. On receiving the required data, the subagent passes the response back on to the master agent, which in turn passes it on to the NMS.

[Figure 6 on page 41](#) shows the communication flow among the NMS, SNMP master agent (`snmpd`), SNMP subagents, Junos OS kernel, and Packet Forwarding Engine.

Figure 6: SNMP Communication Flow



When a significant event, most often an error or a failure, occurs on a network device, the SNMP agent sends notifications to the SNMP manager. SNMP notifications can be sent as traps (unconfirmed notifications) or inform requests (confirmed notifications).

Junos OS supports trap queuing to ensure that traps are not lost because of temporary unavailability of routes. Two types of queues, destination queues and a throttle queue, are formed to ensure delivery of traps and control the trap traffic. On QFX Series products, the maximum size of trap queues (throttle queue plus destination queue) is 40,960 traps. The maximum size of any one queue is 20,480 traps.

Junos OS forms a destination queue when a trap to a particular destination is returned because the host is not reachable, and it adds the subsequent traps to the same destination to the queue. Junos OS checks for availability of routes every 30 seconds, and sends the traps from the destination queue in a round-robin fashion.

If the trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts occur at progressive intervals of 1 minute, 2 minutes, 4 minutes, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is ten. After ten unsuccessful attempts, the destination queue and all the traps in the queue are deleted.

Junos OS also has a throttle mechanism to control the number of traps (throttle threshold) sent during a particular time period (throttle interval). The throttle mechanism ensures consistency in trap traffic, especially when large numbers of traps are generated because of interface status changes. The throttle interval period begins when the first trap arrives at the throttle. All traps within the trap threshold are processed, and the traps beyond the threshold limit are queued. The default throttle threshold is 500 traps, and the throttle interval default is 5 seconds.



NOTE: You cannot configure trap queueing in Junos OS. You cannot view information about trap queues except for what is provided in the system logs.

- Related Documentation**
- [Configuring SNMP on page 121](#)
 - [SNMP MIBs Support on page 56](#)

- [SNMP Traps Support on page 72](#)

Understanding the Implementation of SNMP on the QFabric System

SNMP monitors network devices from a central location. The QFabric system supports the basic SNMP architecture of Junos OS, but its implementation of SNMP differs from that of other devices running Junos OS. This topic provides an overview of the SNMP implementation on the QFabric system.

As in other SNMP systems, the SNMP manager resides on the network management system (NMS) of the network to which the QFabric system belongs. The SNMP agent resides in the QFabric Director software and is responsible for receiving and distributing all traps as well as responding to all the queries of the SNMP manager. For example, traps that are generated by a Node device are sent to the SNMP agent in the Director software, which in turn processes and sends them to the target IP addresses that are defined in the SNMP configuration.



NOTE: In its SNMP implementation, the QFabric system acts as an SNMP proxy server, and requires more time to process SNMP requests than a typical Junos OS device does. The default timeout setting on most SNMP client applications is 3 seconds, which is not enough time for the QFabric system to respond to SNMP requests, so the results of your `mibwalk` command may be incomplete. For this reason, we recommend that you change the SNMP timeout setting to 5 seconds or longer for the QFabric system to complete the responses to your requests.

Support for SNMP on the QFabric system includes:

- Support for the SNMP Version 1 (v1) and v2.



NOTE: Only SNMPv2 traps are supported on the QFabric system.

- Support for the following standard MIBs:
 - RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
 - RFC 1157, *A Simple Network Management Protocol (SNMP)*
 - RFC 1212, *Concise MIB Definitions*
 - RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II* (partial support, including the system group and interfaces group)
 - RFC 1215, *A Convention for Defining Traps for use with the SNMP*
 - RFC 1901, *Introduction to Community-based SNMPv2*
 - RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*

- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*
- RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*
- RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*
- RFC 2233, *The Interfaces Group MIB Using SMIv2*
- RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access) (excluding SNMPv3)
- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access) (excluding SNMPv3)
- RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* (excluding SNMPv3)
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2863, *The Interfaces Group MIB*
- RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework* (excluding SNMPv3)
- RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Framework* (excluding SNMPv3)
- RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (excluding SNMPv3)
- RFC 3413, *Simple Network Management Protocol (SNMP) Applications* (excluding SNMPv3)
- RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
- RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* (excluding SNMPv3)
- RFC 4188, *Definitions of Managed Objects for Bridges*
- RFC 4293, *Management Information Base for the Internet Protocol (IP)*
- RFC 4363b, *Q-Bridge VLAN MIB*

- Support for the following Juniper Networks enterprise-specific MIBs:
 - Chassis MIB (mib-jnx-chassis.txt)
 - Class-of-Service MIB (mib-jnx-cos.txt)
 - Configuration Management MIB (mib-jnx-cfgmngmt.txt)
 - Fabric Chassis MIB (mib-jnx-fabric-chassis.txt)
 - Interface MIB Extensions (mib-jnx-if-extensions.txt)
 - Power Supply Unit MIB (mib-jnx-power-supply-unit.txt)
 - QFabric MIB (mib-jnx-ql-smi.txt)
 - Utility MIB (mib-jnx-util.txt)
- Support for operational mode commands—Limited to the **show snmp statistics** command. You may issue other SNMP requests, including **get**, **get next**, and **walk** requests, by using external SNMP client applications.

- Related Documentation**
- [SNMP MIBs Support on page 56](#)
 - [SNMP Traps Support on page 72](#)

Fabric Chassis MIB

The Juniper Networks enterprise-specific SNMP Fabric Chassis MIB (mib-jnx-fabric-chassis) provides hardware information about the QFabric system and its component devices in a single MIB. The Fabric Chassis MIB is based on the Juniper Networks enterprise-specific Chassis MIB that provides information for individual devices. Unlike the Chassis MIB, the Fabric Chassis MIB represents the QFabric system component devices as part of the QFabric system. Only the information from the Fabric Chassis MIB (and not from individual Chassis MIBs) is available to SNMP management clients of the QFabric system.

The Fabric Chassis MIB uses the basic information structure of the Chassis MIB, but adds another level of indexing that provides detailed information about QFabric system devices. Each physical device in a QFabric system (such as a Node device or an Interconnect device) is represented with its hardware components, including the power supply, fans, and front and rear cards.

As in other SNMP systems, the SNMP manager resides on the network management system (NMS) of the network to which the QFabric system belongs. The SNMP agent (snmpd) resides in the QFabric system Director software and is responsible for receiving and distributing all traps as well as responding to all queries from the SNMP manager. In addition, there is an SNMP subagent running in the Routing Engine of each Node group and Interconnect device. The SNMP subagent manages the information about the component device, and that information is communicated to the SNMP agent in the Director software as needed. Traps that are generated by a Node device are sent to the SNMP agent in the Director software, which in turn processes and sends them to the target IP addresses that are defined in the SNMP configuration.

Table 5 on page 45 describes the tables and objects in the Fabric Chassis MIB.

Table 5: Fabric Chassis MIB Tables and Objects

Table or Object Name	Root OID	Description
Tables with Counterparts in the Chassis MIB		
jnxFabricContainersTable	1.3.6.1.4.1.2636.3.42.2.2.2	<p>Provides information about different types of containers in QFabric system devices.</p> <ul style="list-style-type: none"> Containers for Interconnect devices include fan trays, power supply units, control boards, and so on. Containers for Node devices include fan trays, power supply units, Flexible PIC Concentrator (FPC), PICs, and so on. Containers for the Director devices include CPU, memory, fan trays, power supply units, and hard disks. The containers have a non-hierarchical or flat structure, and components in them are organized as siblings to each other.
jnxFabricContentsTable	1.3.6.1.4.1.2636.3.42.2.2.3	<p>Contains contents that are present across all devices represented in the jnxFabricDeviceTable object. This table includes all field replaceable units (FRUs) and non-FRUs for QFabric system devices.</p> <ul style="list-style-type: none"> Contents in the Interconnect devices include fan trays and control boards. Contents in the Node devices include fan trays and power supply units. Contents in the Director devices include CPUs, memory, fan trays, power supply units, and hard disks, but do not include network interface cards (NICs).
jnxFabricFilledTable	1.3.6.1.4.1.2636.3.42.2.2.4	<p>Shows the status of containers in QFabric devices. The jnxFabricFilledState object represents the state of the component: (1) unknown, (2) empty, or (3) filled.</p> <p>NOTE: The jnxFabricFilledTable object does not contain information about the Director group.</p>
jnxFabricOperatingTable	1.3.6.1.4.1.2636.3.42.2.2.5	<p>Represents different operating parameters for the contents that are populated in the jnxFabricContentsTable object.</p> <ul style="list-style-type: none"> Contents in each Node device and Interconnect device include fan trays, power supply units, FPC, PIC, and Routing Engine. Contents in the Director device include CPUs, memory, fan trays, power supply units, and hard disks, but do not include network interface cards (NICs). <p>The jnxFabricOperatingState object provides the state of the device: (1) unknown, (2) running, (3) ready, (4) reset, (5) runningAtFullSpeed (for fans only), (6) down, (6) off (for power supply units), or (7) standby.</p>

Table 5: Fabric Chassis MIB Tables and Objects (*continued*)

Table or Object Name	Root OID	Description
jnxFabricRedundancyTable	1.3.6.1.4.1.2636.3.42.2.2.6	<p>Represents the redundancy information that is available at different subsystem levels across the QFabric system. Information about the Routing Engines in Node devices is included, but there are no corresponding entries for Interconnect devices in this table. The jnxFabricRedundancyState object indicates the state of the subsystem: (1) unknown, (2) master, (3) backup, or (4) disabled.</p> <p>NOTE: Information about redundant Director devices, virtual machines (VMs) within Director groups, and Virtual Chassis devices is not available at this time.</p>
jnxFabricFruTable	1.3.6.1.4.1.2636.3.42.2.2.7	<p>Contains all FRUs for the QFabric system in the jnxFabricDeviceTable table. The FRUs are listed regardless of whether or not they are installed or online. The jnxFabricFruState object represents the state of the FRU, including online, offline, or empty, and so on. This table also contains information about each FRU, such as name, type, temperature, time last powered on, and time last powered off.</p> <p>NOTE: The jnxFabricFruTable table does not include network interface cards (NICs) on Director devices.</p>
Table Specific to the Fabric Chassis MIB		
jnxFabricDeviceTable	1.3.6.1.4.1.2636.3.42.2.2.1	<p>Contains information about all devices in the QFabric system. This table organizes scalar variables represented in the Chassis MIB into a table format for the QFabric system component devices. Columns in this table include device information such as model, device alias, and serial number. The jnxFabricDeviceIndex identifies each QFabric system device (Node device, Interconnect device, and Director device).</p> <p>NOTE: At this time, information about the Virtual Chassis is not available.</p> <p>NOTE: The following objects are not supported:</p> <ul style="list-style-type: none"> jnxFabricDeviceEntryRevision jnxFabricDeviceEntryFirmwareRevision jnxFabricDeviceEntryKernelMemoryUsedPercent

Scalar Variables

Table 5: Fabric Chassis MIB Tables and Objects (*continued*)

Table or Object Name	Root OID	Description
<p>The following scalar variables are supported:</p> <ul style="list-style-type: none"> • jnxFabricClass • jnxFabricDescr • jnxFabricSerialNo • jnxFabricRevision • jnxFabricLastInstalled • jnxFabricContentsLastChange • jnxFabricFilledLastChange 	1.3.6.1.4.1.2636.3.42.2.1	<p>Describe the QFabric system as a whole.</p> <p>NOTE: The jnxFabricFirmwareRevision scalar variable is not supported at this time.</p>

Table 6 on page 47 describes the SNMPv2 traps that are defined in the Fabric Chassis MIB.



NOTE: Only SNMPv2 traps are supported on the QFabric system.

Table 6: Fabric Chassis MIB SNMPv2 Traps

Trap Group and Name	Root OID	Description
<p>jnxFabricChassisTraps group—Includes the following traps:</p> <ul style="list-style-type: none"> • jnxFabricPowerSupplyFailure • jnxFabricFanFailure • jnxFabricOverTemperature • jnxFabricRedundancySwitchover • jnxFabricFruRemoval • jnxFabricFruInsertion • jnxFabricFruPowerOff • jnxFabricFruPowerOn • jnxFabricFruFailed • jnxFabricFruOffline • jnxFabricFruOnline • jnxFabricFruCheck • jnxFabricFEBSwitchover • jnxFabricHardDiskFailed • jnxFabricHardDiskMissing • jnxFabricBootFromBackup 	1.3.6.1.4.1.2636.4.19	<p>Indicates an alarm condition.</p> <p>NOTE: Hardware events on the Director group are detected by scanning. As a result, a trap may not be generated until up to 30 seconds after the event has occurred.</p> <p>NOTE: The software does not distinguish between the fan removal and fan failure events on the Director group. In each case, both the jnxFabricFanFailure and jnxFabricFruFailed traps are generated.</p>

Table 6: Fabric Chassis MIB SNMPv2 Traps (continued)

Trap Group and Name	Root OID	Description
<p>jnxFabricChassisOKTraps group—Includes the following traps:</p> <ul style="list-style-type: none"> • jnxFabricPowerSupplyOK • jnxFabricFanOK • jnxFabricTemperatureOK • jnxFabricFruOK 	1.3.6.1.4.1.2636.4.20	Indicates an alarm cleared condition.

For more information, see the Fabric Chassis MIB at:

http://www.juniper.net/techpubs/en_US/junos13.1/topics/reference/mibs/mib-jnx-fabric-chassis.txt

**Related
Documentation**

- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
- [Chassis MIBs](#)

Utility MIB

The Juniper Networks enterprise-specific Utility MIB, whose object ID is {jnxUtilMibRoot 1}, defines objects for counters, integers, and strings. The Utility MIB contains one table for each of the following five data types:

- 32-bit counters
- 64-bit counters
- Signed integers
- Unsigned integers
- Octet strings

Each data type has an arbitrary ASCII name, which is defined when the data is populated, and a timestamp that shows the last time when the data instance was modified. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos14.1/topics/reference/mibs/mib-jnx-util.txt.

For information about the enterprise-specific Utility MIB objects, see the following topics:

- *jnxUtilCounter32Table*
- *jnxUtilCounter64Table*
- *jnxUtilIntegerTable*
- *jnxUtilUintTable*
- *jnxUtilStringTable*

**Related
Documentation**

- [Juniper Networks Enterprise-Specific MIBs](#)

- *Juniper Networks Enterprise-Specific MIBs*
- *Standard SNMP MIBs Supported by Junos OS*
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)

SNMPv3 Overview

The QFX3500 switch supports SNMP version 3 (SNMPv3). SNMPv3 enhances the functionality of SNMPv1 and SNMPv2c by supporting user authentication and data encryption. SNMPv3 uses the user-based security model (USM) to provide security for SNMP messages, and the view-based access control model (VACM) for user access control.

SNMPv3 features include:

- With USM, the SNMP messages between the SNMP manager and the agent can have the message source authenticated and the data integrity checked. USM reduces messaging delays and message replays by enforcing timeout limits and by checking for duplicate message request IDs.
- VACM complements USM by providing user access control for SNMP queries to the agent. You define access privileges that you wish to extend to a group of one or more users. Access privileges are determined by the security model parameters (**usm**, **v1**, or **v2**) and security level parameters (**authentication**, **privacy**, or **none**). For each security level, you must associate one MIB view for the group. Associating a MIB view with a group grants the read, write, or notify permission to a set of MIB objects for the group.
- You configure security parameters for each user, including the username, authentication type and authentication password, and privacy type and privacy password. The username given to each user is in a format that is dependent on the security model configured for that user.
- To ensure messaging security, another type of username, called the security name, is included in the messaging data that is sent between the local SNMP server and the destination SNMP server. Each user name is mapped to a security name, but the security name is in a format that is independent of the security model.
- Trap entries in SNMPv3 are created by configuring the notify, notify filter, target address, and target parameters. The **notify** statement specifies the type of notification (trap) and contains a single tag that defines a set of target addresses to receive a trap. The notify filter defines access to a collection of trap object identifiers (OIDs). The target address defines the address of an SNMP management application and other attributes used in sending notifications. Target parameters define the message processing and security parameters used in sending notifications to a particular target.

Related Documentation

- [Assigning a Security Name to a Group on page 136](#)
- [Configuring Access Privileges for a Group on page 134](#)
- [Configuring SNMP Informs on page 138](#)
- [Creating SNMPv3 Users on page 133](#)

Minimum SNMPv3 Configuration on a Device Running Junos OS

To configure the minimum requirements for SNMPv3, include the following statements at the `[edit snmp v3]` and `[edit snmp]` hierarchy levels:



NOTE: You must configure at least one view (notify, read, or write) at the `[edit snmp view-name]` hierarchy level.

```
[edit snmp]
view view-name {
  oid object-identifier (include | exclude);
}
[edit snmp v3]
notify name {
  tag tag-name;
}
notify-filter profile-name {
  oid object-identifier (include | exclude);
}
snmp-community community-index {
  security-name security-name;
}
target-address target-address-name {
  address address;
  target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
usm {
  local-engine {
    user username {
    }
  }
}
vacm {
  access {
    group group-name {
      (default-context-prefix | context-prefix context-prefix){
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
}
```



```

    }
  }
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}
}

```

Related Documentation

- [Creating SNMPv3 Users on page 133](#)
- [Configuring MIB Views on page 129](#)
- *Defining Access Privileges for an SNMP Group*
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 137](#)
- [Configuring SNMP Informs on page 138](#)
- *Complete SNMPv3 Configuration Statements*
- *Example: SNMPv3 Configuration*

Understanding RMON

- [RMON Overview on page 51](#)
- [Alarm Thresholds and Events on page 52](#)

RMON Overview

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

An operational support system (OSS) or a fault-monitoring system can be used to automatically monitor events that track many different metrics, including performance, availability, faults, and environmental data. For example, an administrator might want to know when the internal temperature of a chassis has risen above a configured threshold, which might indicate that a chassis fan tray is faulty, the chassis air flow is impeded, or the facility cooling system in the vicinity of the chassis is not operating normally.

The RMON MIB also defines tables that store various statistics for Ethernet interfaces, including the **etherStatsTable** and the **etherHistoryTable**. The **etherStatsTable** contains cumulative real-time statistics for Ethernet interfaces, such as the number of unicast, multicast, and broadcast packets received on an interface. The **etherHistoryTable** maintains a historical sample of statistics for Ethernet interfaces. The control of the **etherHistoryTable**, including the interfaces to track and the sampling interval, is defined by the RMON **historyControlTable**.

To enable RMON alarms, you perform the following steps:

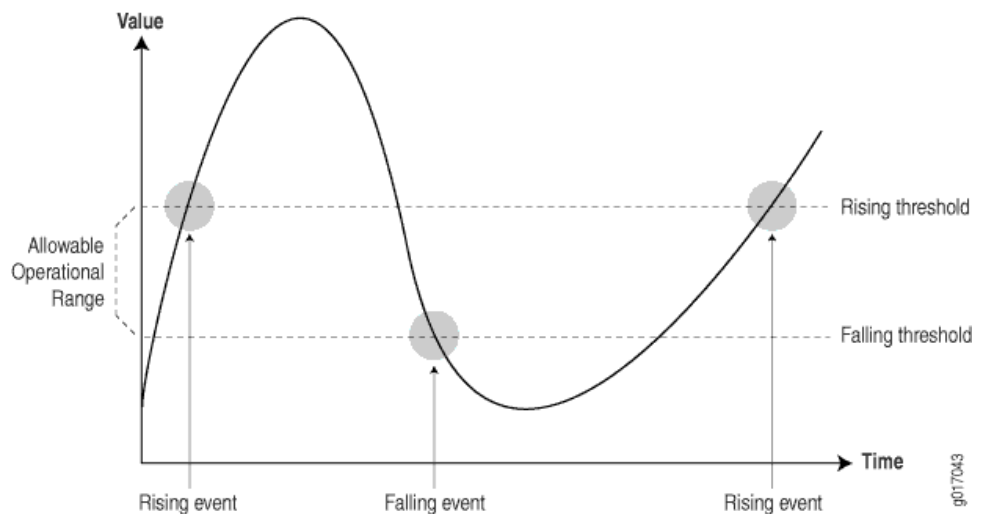
1. Configure SNMP, including trap groups. You configure SNMP at the `[edit snmp]` hierarchy level.
2. Configure rising and falling events in the `eventTable`, including the event types and trap groups. You can also configure events using the CLI at the `[edit snmp rmon event]` hierarchy level.
3. Configure alarms in the `alarmTable`, including the variables to monitor, rising and falling thresholds, the sampling types and intervals, and the corresponding events to generate when alarms occur. You can also configure alarms using the CLI at the `[edit snmp rmon alarm]` hierarchy level.

Extensions to the `alarmTable` are defined in the Juniper Networks enterprise-specific MIB `jnxRmon` (`mib-jnx-rmon.txt`).

Alarm Thresholds and Events

By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range (see [Figure 7 on page 52](#)).

Figure 7: Setting Thresholds



Events are only generated when the alarm threshold is first crossed in any one direction rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs. This considerably reduces the quantity of events that are produced by the system, making it easier for operations staff to react when events do occur.

Before you configure remote monitoring, you should identify what variables need to be monitored and their allowable operational range. This requires some period of baselining to determine the allowable operational ranges. An initial baseline period of at least

3 months is not unusual when you first identify the operational ranges and define thresholds, but baseline monitoring should continue over the life span of each monitored variable.

Related Documentation

- [Configuring RMON Alarms and Events on page 130](#)
- [Juniper Networks Enterprise-Specific MIBs](#)
- [RMON MIB Event, Alarm, Log, and History Control Tables on page 53](#)

RMON MIB Event, Alarm, Log, and History Control Tables

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

[Table 7 on page 53](#) provides each field in the RMON eventTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the `[edit snmp rmon]` hierarchy level.

Table 7: RMON Event Table

Field	Description	Statement [edit snmp rmon]
eventDescription	Text description of this event.	description
eventType	Type of event (for example, log, trap, or log and trap).	type
eventCommunity	Trap group to which to send this event, as defined in the Junos OS configuration. (This is not the same as the SNMP community.)	community
eventOwner	Entity (for example, manager) that created this event.	—
eventStatus	Status of this row (for example, valid, invalid, or createRequest).	—

[Table 8 on page 53](#) provides each field in the RMON alarmTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the `[edit snmp rmon]` hierarchy level.

Table 8: RMON Alarm Table

Field	Description	Statement [edit snmp rmon]
alarmStatus	Status of this row (for example, valid, invalid, or createRequest)	—
alarmInterval	Sampling period (in seconds) of the monitored variable	interval
alarmVariable	Object identifier (OID) and instance of the variable to be monitored	—

Table 8: RMON Alarm Table (*continued*)

Field	Description	Statement [edit snmp rmon]
alarmValue	Actual value of the sampled variable	—
alarmSampleType	Sample type (absolute or delta changes)	sample-type
alarmStartupAlarm	Initial alarm (rising, falling, or either)	startup-alarm
alarmRisingThreshold	Rising threshold against which to compare the value	rising-threshold
alarmFallingThreshold	Falling threshold against which to compare the value	falling-threshold
alarmRisingEventIndex	Index (row) of the rising event in the event table	rising-event-index
alarmFallingEventIndex	Index (row) of the falling event in the event table	falling-event-index

Table 9 on page 54 provides each field in the jnxRmon jnxRmonAlarmTable, which is an extension to the RMON alarmTable. You can troubleshoot the RMON agent, rmopd, that runs on a switch by inspecting the contents of the jnxRmonAlarmTable object.

Table 9: jnxRmon Alarm Table

Field	Description
jnxRmonAlarmGetFailCnt	Number of times the internal Get request for the variable failed
jnxRmonAlarmGetFailTime	Value of the sysUpTime object when the last failure occurred
jnxRmonAlarmGetFailReason	Reason why the Get request failed
jnxRmonAlarmGetOkTime	Value of the sysUpTime object when the variable moved out of failure state
jnxRmonAlarmState	Status of this alarm entry

Table 10 on page 54 provides each field in the RMON historyControlTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [edit snmp rmon history] hierarchy level. The historyControlTable controls the RMON etherHistoryTable.

Table 10: RMON History Control Table

Field	Description	Statement [edit snmp rmon history]
historyControlDataSource	Identifies the source of the data for which historical data was collected.	interface

Table 10: RMON History Control Table (*continued*)

Field	Description	Statement [edit snmp rmon history]
historyControlBucketsRequested	Requested number of discrete time intervals over which data is to be saved.	bucket-size
historyControlBucketsGranted	Number of discrete sampling intervals over which data is to be saved.	—
historyControlInterval	Interval, in seconds, over which the data is sampled for each bucket.	interval
historyControlOwner	Entity that configured this entry.	owner
historyControlStatus	Status of this entry.	—

Related Documentation

- [Configuring RMON Alarms and Events on page 130](#)
- [Juniper Networks Enterprise-Specific MIBs](#)
- [Understanding RMON on page 51](#)

Understanding Health Monitoring

Health monitoring is an SNMP feature that extends the RMON alarm infrastructure to provide monitoring for a predefined set of objects (such as file system usage, CPU usage, and memory usage), and for Junos OS processes.

You enable the health monitor feature using the **health-monitor** statement at the **[edit snmp]** hierarchy level. You can also configure health monitor parameters such as a falling threshold, rising threshold, and interval. If the value of a monitored object exceeds the rising or falling threshold, an alarm is triggered and an event may be logged.

The falling threshold is the lower threshold for the monitored object instance. The rising threshold is the upper threshold for the monitored object instance. Each threshold is expressed as a percentage of the maximum possible value. The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

Events are only generated when a threshold is first crossed in any one direction, rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs.

System log entries for health monitor events have a corresponding HEALTHMONITOR tag and not a generic SNMPD_RMON_EVENTLOG tag. However, the health monitor sends generic RMON risingThreshold and fallingThreshold traps. You can use the **show snmp health-monitor** operational command to view information about health monitor alarms and logs.

When you configure the health monitor, monitoring information for certain object instances is available, as shown in [Table 11 on page 56](#).

Table 11: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed.1	Monitors the /dev/ad0s1a : file system on the switch. This is the root file system mounted on / .
jnxHrStoragePercentUsed.2	Monitors the /dev/ad0s1e : file system on the switch. This is the configuration file system mounted on /config .
jnxOperatingCPU (RE0)	Monitors CPU usage by the Routing Engine (RE0).
jnxOperatingBuffer (RE0)	Monitors the amount of memory available on the Routing Engine (RE0).
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS process. Multiple instances of the same process are monitored and indexed separately.

- Related Documentation**
- [Configuring Health Monitoring on page 132](#)
 - [falling-threshold \(Health Monitor\) on page 283](#)
 - [interval \(Health Monitor\) on page 293](#)
 - [rising-threshold \(Health Monitor\) on page 316](#)
 - [show snmp health-monitor on page 424](#)

SNMP MIBs Support

The QFX Series standalone switches, QFX Series Virtual Chassis, QFabric systems, and OCX Series support standard MIBs and Juniper Networks enterprise-specific MIBs.

For more information, see:

- [MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series on page 56](#)
- [MIBs Supported on QFabric Systems on page 66](#)

MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

The QFX Series standalone switches, QFX Series Virtual Chassis, and OCX Series support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

- [Table 12 on page 57](#) for standard MIBs.

- [Table 13 on page 62](#) for Juniper Networks enterprise-specific MIBs.

Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

RFC	Additional Information
IEEE 802.1ab section 12.1, <i>Link Layer Discovery Protocol (LLDP) MIB</i>	Supported tables and objects: <ul style="list-style-type: none"> • lldpRemManAddrOID • lldpLocManAddrOID • lldpReinitDelay • lldpNotificationInterval • lldpStatsRxPortFramesDiscardedTotal • lldpStatsRxPortFramesError • lldpStatsRxPortTLVsDiscardedTotal • lldpStatsRxPortTLVsUnrecognizedTotal • lldpStatsRxPortAgeoutsTotal
IEEE 802.3ad, <i>Aggregation of Multiple Link Segments</i>	The following tables and objects are supported: <ul style="list-style-type: none"> • dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable • dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount) • dot3adTablesLastChanged
RFC 1155, <i>Structure and Identification of Management Information for TCP/IP-based Internets</i>	—
RFC 1157, <i>A Simple Network Management Protocol (SNMP)</i>	—
RFC 1212, <i>Concise MIB Definitions</i>	—
RFC 1213, <i>Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II</i>	The following areas are supported: <ul style="list-style-type: none"> • MIB II and its SNMP version 2 derivatives, including: <ul style="list-style-type: none"> • Statistics counters • IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, <i>IP Forwarding Table MIB</i>) • ipAddrTable • SNMP management • Interface management • SNMPv1 Get, GetNext requests, and SNMPv2 GetBulk request • Junos OS-specific secured access list • Master configuration keywords • Reconfigurations upon SIGHUP

Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

RFC	Additional Information
RFC 1215, <i>A Convention for Defining Traps for use with the SNMP</i>	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, <i>Definitions of Managed Objects for Bridges</i>	—
RFC 1657, <i>Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2</i>	—
RFC 1850, <i>OSPF Version 2 Management Information Base</i>	<p>The following table, objects, and traps are not supported:</p> <ul style="list-style-type: none"> • Host Table • ospfOriginateNewLsas and ospfRxNewLsas objects • ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow traps
RFC 1901, <i>Introduction to Community-based SNMPv2</i>	—
RFC 1905, <i>Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	—
RFC 1907, <i>Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	—
RFC 2011, <i>SNMPv2 Management Information Base for the Internet Protocol Using SMIv2</i>	—
RFC 2012, <i>SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2</i>	—
RFC 2013, <i>SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2</i>	—
RFC 2233, <i>The Interfaces Group MIB Using SMIv2</i>	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2287, <i>Definitions of System-Level Managed Objects for Applications</i>	<p>The following objects are supported:</p> <ul style="list-style-type: none"> • sysApplInstallPkgTable • sysApplInstallElmtTable • sysApplElmtRunTable • sysApplMapTable

Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

RFC	Additional Information
RFC 2570, <i>Introduction to Version 3 of the Internet-standard Network Management Framework</i>	—
RFC 2571, <i>An Architecture for Describing SNMP Management Frameworks</i> (read-only access)	NOTE: RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i> (read-only access)	NOTE: RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.
RFC 2576, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	NOTE: RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, <i>Structure of Management Information Version 2 (SMIv2)</i>	—
RFC 2579, <i>Textual Conventions for SMIv2</i>	—
RFC 2580, <i>Conformance Statements for SMIv2</i>	—
RFC 2665, <i>Definitions of Managed Objects for the Ethernet-like Interface Types</i>	—
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i>	Support does not include row creation, the Set operation, and the vrrpStatsPacketLengthErrors object.
RFC 2790, <i>Host Resources MIB</i>	Support is limited to the following objects: <ul style="list-style-type: none"> Only hrStorageTable. The file systems <code>/</code>, <code>/config</code>, <code>/var</code>, and <code>/tmp</code> always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change. Only the objects of the hrSystem and hrSWInstalled groups.
RFC 2819, <i>Remote Network Monitoring Management Information Base</i>	The following objects are supported: <ul style="list-style-type: none"> etherStatsTable (for Ethernet interfaces only), alarmTable, eventTable, and logTable. historyControlTable and etherHistoryTable (except the etherHistoryUtilization object).
RFC 2863, <i>The Interfaces Group MIB</i>	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2932, <i>IPv4 Multicast Routing MIB</i>	—

Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

RFC	Additional Information
RFC 2933, <i>Internet Group Management Protocol (IGMP) MIB</i>	—
RFC 2934, <i>Protocol Independent Multicast MIB for IPv4</i>	In Junos OS, RFC 2934 is implemented based on a draft version, <i>pimmib.mib</i> , of the now standard RFC.
RFC 3410, <i>Introduction and Applicability Statements for Internet Standard Management Framework</i>	—
RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i>	NOTE: RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3413, <i>Simple Network Management Protocol (SNMP) Applications</i>	All MIBs are supported except for the Proxy MIB.
RFC 3414, <i>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</i>	—
RFC 3415, <i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>	—
RFC 3416, <i>Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.
RFC 3417, <i>Transport Mappings for the Simple Network Management Protocol (SNMP)</i>	—
RFC 3418, <i>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.
RFC 3584, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	—
RFC 3826, <i>The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model</i>	—

Table 12: Standard MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

RFC	Additional Information
RFC 4188, <i>Definitions of Managed Objects for Bridges</i>	<p>The QFX3500 and QFX3600 switches support 802.1D STP (1998) and the following subtrees and objects only:</p> <ul style="list-style-type: none"> dot1dTp subtree—dot1dTpFdbAddress, dot1dTpFdbPort, and dot1dTpFdbStatus objects from the dot1dTpFdbTable table. dot1dBase subtree—dot1dBasePort and dot1dBasePortIfIndex objects from the dot1dBasePortTable table. <p>NOTE: On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (RFC 4363b, <i>Q-Bridge VLAN MIB</i>) when you issue the show snmp mib walk command.</p> <p>Not supported on OCX Series devices.</p>
RFC 4293, <i>Management Information Base for the Internet Protocol (IP)</i>	Supports the ipAddrTable table only.
RFC 4318, <i>Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol</i>	<p>Supports 802.1w and 802.1t extensions for RSTP.</p> <p>Not supported on OCX Series devices.</p>
RFC 4363b, <i>Q-Bridge VLAN MIB</i>	<p>NOTE: On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table (RFC 4188, <i>Definitions of Managed Objects for Bridges</i>) is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (in this MIB) when you issue the show snmp mib walk command.</p> <p>Not supported on OCX Series devices.</p>
RFC 4444, <i>IS-IS MIB</i>	—
Internet Assigned Numbers Authority, <i>IANAiftype Textual Convention MIB</i> (referenced by RFC 2233)	See http://www.iana.org/assignments/ianaiftype-mib .
Internet draft draft-reeder-snmppv3-usm-3desede-00.txt, <i>Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode</i>	—
Internet draft draft-ietf-idmr-igmp-mib-13.txt, <i>Internet Group Management Protocol (IGMP) MIB</i>	—
ESO Consortium MIB	<p>NOTE: The ESO Consortium MIB has been replaced by RFC 3826. See http://www.snmp.com/eso/.</p>

Table 13: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

MIB	Description
Alarm MIB (mib-jnx-chassis-alarm)	<p>Provides support for alarms from the switch.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-chassis-alarm.txt.</p> <p>For more information, see <i>Alarm MIB</i>.</p>
Analyzer MIB (mib-jnx-analyzer)	<p>Contains analyzer and remote analyzer data related to port mirroring.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-analyzer.txt.</p> <p>For more information, see <i>Analyzer MIB</i>.</p> <p>Not supported on OCX Series devices.</p>
Chassis MIB (mib-jnx-chassis)	<p>Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and airflow) and inventory support for the chassis, Flexible PIC Concentrators (FPCs), and PICs.</p> <p>NOTE: The jnxLEDTable table has been deprecated.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-chassis.txt.</p> <p>For more information, see <i>Chassis MIBs</i>.</p>
Chassis Definitions for Router Model MIB (mib-jnx-chas-defines)	<p>Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify routing and switching platforms and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-chas-defines.txt.</p> <p>For more information, see <i>Chassis MIBs</i>.</p>
Class-of-Service MIB (mib-jnx-cos)	<p>Provides support for monitoring interface output queue statistics per interface and per forwarding class.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-cos.txt.</p> <p>For more information, see <i>Class-of-Service MIB</i>.</p>

Table 13: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

MIB	Description
Configuration Management MIB (mib-jnx-cfgmgt)	<p>Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made.</p> <p>A history of the last 32 configuration changes is kept in jnxCmChgEventTable.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-cfgmgt.txt.</p> <p>For more information, see <i>Configuration Management MIB</i>.</p>
Ethernet MAC MIB (mib-jnx-mac)	<p>Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, inoctets, inframes, outoctets, and outframes on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-mac.txt.</p> <p>For more information, see <i>Ethernet MAC MIB</i>.</p> <p>Not supported on OCX Series devices.</p>
Event MIB (mib-jnx-event)	<p>Defines a generic trap that can be generated using an operations script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found.</p> <p>In Junos OS release 13.2X51-D10 or later, if you configured an event policy to raise a trap when a new SNMP trap target is added, the SNMPD_TRAP_TARGET_ADD_NOTICE trap is generated with information about the new target.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-event.txt.</p> <p>For more information, see <i>Event MIB</i>.</p>
Firewall MIB (mib-jnx-firewall)	<p>Provides support for monitoring firewall filter counters.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-firewall.txt.</p> <p>For more information, see <i>Firewall MIB</i>.</p>

Table 13: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

MIB	Description
Host Resources MIB (mib-jnx-hostresources)	<p>Extends the hrStorageTable object, providing a measure of the usage of each file system on the switch as a percentage. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-hostresources.txt.</p> <p>For more information, see <i>Host Resources MIB</i>.</p>
Interface MIB (Extensions) (mib-jnx-if-extensions)	<p>Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-if-extensions.txt.</p> <p>For more information, see <i>Interface MIB</i>.</p>
MPLS MIB (mib-jnx-mpls)	<p>Provides MPLS information and defines MPLS notifications.</p> <p>NOTE: This MIB is not supported on the QFX5100 switch.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-mpls.txt.</p> <p>For more information, see <i>MPLS MIB</i>.</p>
MPLS LDP MIB (mib-jnx-mpls-ldp)	<p>Contains object definitions as described in RFC 3815, <i>Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)</i>.</p> <p>NOTE: This MIB is not supported on the QFX5100 switch.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-mpls-ldp.txt.</p> <p>For more information, see <i>MPLS LDP MIB</i>.</p>
Ping MIB (mib-jnx-ping)	<p>Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in pingCtlTable of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-ping.txt.</p> <p>For more information, see <i>PING MIB</i>.</p>

Table 13: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

MIB	Description
RMON Events and Alarms MIB (mib-jnx-rmon)	<p>Supports Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments the alarmTable object with additional information about each alarm. Two additional traps are also defined to indicate when problems are encountered with an alarm.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-rmon.txt.</p> <p>For more information, see <i>RMON Events and Alarms MIB</i>.</p>
Structure of Management Information MIB (mib-jnx-smi)	<p>Explains how the Juniper Networks enterprise-specific MIBs are structured.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-smi.txt.</p> <p>For more information, see <i>Structure of Management Information MIB</i>.</p>
System Log MIB (mib-jnx-syslog)	<p>Enables notification of an SNMP trap-based application when an important system log message occurs.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-syslog.txt.</p> <p>For more information, see <i>System Log MIB</i>.</p>
Utility MIB (mib-jnx-util)	<p>Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-util.txt.</p> <p>For more information, see “Utility MIB” on page 48 and “Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage” on page 186.</p>
VLAN MIB (mib-jnx-vlan)	<p>Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-vlan.txt.</p> <p>For more information, see <i>VLAN MIB</i>.</p> <p>Not supported on OCX Series devices.</p>

MIBs Supported on QFabric Systems

The QFabric systems support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

- [Table 14 on page 66](#) for standard MIBs.
- [Table 15 on page 70](#) for Juniper Networks enterprise-specific MIBs.

Table 14: Standard MIBs Supported on QFabric Systems

RFC	Additional Information
RFC 1155, <i>Structure and Identification of Management Information for TCP/IP-based Internets</i>	—
RFC 1157, <i>A Simple Network Management Protocol (SNMP)</i>	—
RFC 1212, <i>Concise MIB Definitions</i>	—
RFC 1213, <i>Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II</i>	<p>The following areas are supported:</p> <ul style="list-style-type: none"> • MIB II and its SNMP version 2 derivatives, including: <ul style="list-style-type: none"> • Statistics counters • IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, <i>IP Forwarding Table MIB</i>) • ipAddrTable • SNMP management • Interface management • SNMPv1 Get, GetNext requests, and version 2 GetBulk request • Junos OS-specific secured access list • Master configuration keywords • Reconfigurations upon SIGHUP
RFC 1215, <i>A Convention for Defining Traps for use with the SNMP</i>	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, <i>Definitions of Managed Objects for Bridges</i>	—
RFC 1901, <i>Introduction to Community-based SNMPv2</i>	—
RFC 1905, <i>Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	—
RFC 1907, <i>Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	—

Table 14: Standard MIBs Supported on QFabric Systems (*continued*)

RFC	Additional Information
RFC 2011, <i>SNMPv2 Management Information Base for the Internet Protocol Using SMIv2</i>	NOTE: On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.
RFC 2012, <i>SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2</i>	—
RFC 2013, <i>SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2</i>	—
RFC 2233, <i>The Interfaces Group MIB Using SMIv2</i>	<p>NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.</p> <p>NOTE: The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.</p>
RFC 2571, <i>An Architecture for Describing SNMP Management Frameworks</i> (read-only access)	NOTE: RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i> (read-only access)	NOTE: RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.
RFC 2576, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	NOTE: RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, <i>Structure of Management Information Version 2 (SMIv2)</i>	—
RFC 2579, <i>Textual Conventions for SMIv2</i>	—
RFC 2580, <i>Conformance Statements for SMIv2</i>	—

Table 14: Standard MIBs Supported on QFabric Systems (*continued*)

RFC	Additional Information
RFC 2665, <i>Definitions of Managed Objects for the Ethernet-like Interface Types</i>	<p>The QFabric system supports the following tables only:</p> <ul style="list-style-type: none"> dot3StatsTable—There is one row with statistics for each Ethernet-like interface in the QFabric system. The dot3StatsIndex is an interface index that is unique across the system. dot3ControlTable—There is one row in this table for each Ethernet-like interface in the QFabric system that implements the MAC control sublayer. OIDs supported are dot3ControlFunctionsSupported and dot3ControlInUnknownOpcode. dot3PauseTable—There is one row in this table for each Ethernet-like interface in the QFabric system that supports the MAC control PAUSE function. OIDs supported are dot3PauseAdminMode, dot3PauseOperMode, dot3InPauseFrames, and dot3OutPauseFrames. <p>NOTE: Scalar variables are not supported on the QFabric system.</p>
RFC 2863, <i>The Interfaces Group MIB</i>	<p>NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.</p> <p>NOTE: The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.</p>
RFC 2933, <i>Internet Group Management Protocol (IGMP) MIB</i>	—
RFC 3410, <i>Introduction and Applicability Statements for Internet Standard Management Framework</i>	—
RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i>	NOTE: RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3416, <i>Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.
RFC 3417, <i>Transport Mappings for the Simple Network Management Protocol (SNMP)</i>	—
RFC 3418, <i>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</i>	NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.
RFC 3584, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	—

Table 14: Standard MIBs Supported on QFabric Systems (*continued*)

RFC	Additional Information
RFC 4188, <i>Definitions of Managed Objects for Bridges</i>	<p>The QFabric system support is limited to the following objects:</p> <ul style="list-style-type: none"> Under the dot1dBase OID, the dot1dBasePortTable table supports only the first two columns in the table: dot1dBasePort and dot1dBasePortIfIndex. The system does not implement the optional traps supporting dot1dNotifications (dot1dBridge 0). Under the dot1dStp OID, supports only the dot1dStpPortTable table. Does not support the scalar variables under dot1dStp. The system does not support scalar variables under dot1dTp, but under that, the dot1dTpFdbTable table is supported (dot1dBridge 4). For OIDs with tables support only, scalar values that are returned by the SNMP agent may not be meaningful and are therefore not recommended for use. <p>Not supported on OCX Series devices.</p>
RFC 4293, <i>Management Information Base for the Internet Protocol (IP)</i>	<p>Supports the ipAddrTable table only.</p> <p>On the QFabric system, supported objects in the ipAddrTable table include: ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask, ipAdEntBcastAddr, and ipAdEntReasmMaxSize.</p> <p>NOTE: On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.</p>
RFC 4363b, <i>Q-Bridge VLAN MIB</i>	<p>The QFabric system supports the following tables only:</p> <ul style="list-style-type: none"> dot1qTpFdbTable dot1qVlanStaticTable dot1qPortVlanTable dot1qFdbTable <p>Not supported on OCX Series devices.</p>



NOTE: QFabric-specific MIBs are not supported on OCX Series devices.

Table 15: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems

MIB	Description
Analyzer MIB (mib-jnx-analyzer)	<p>Contains analyzer and remote analyzer data related to port mirroring.</p> <p>The QFabric system supports:</p> <ul style="list-style-type: none"> Analyzer table—jnxAnalyzerName, jnxMirroringRatio, jnxLossPriority. Analyzer input table—jnxAnalyzerInputValue, jnxAnalyzerInputOption, jnxAnalyzerInputType. Analyzer output table—jnxAnalyzerOutputValue, jnxAnalyzerOutputType. <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-analyzer.txt.</p> <p>For more information, see <i>Analyzer MIB</i>.</p>
Chassis MIB (mib-jnx-chassis)	<p>NOTE: The Chassis MIB has been deprecated for the QFabric system. We recommend that you use the Fabric Chassis MIB (mib-jnx-fabric-chassis) for information about the QFabric system.</p>
Class-of-Service MIB (mib-jnx-cos)	<p>Provides support for monitoring interface output queue statistics per interface and per forwarding class.</p> <p>The QFabric system supports the following tables and objects:</p> <ul style="list-style-type: none"> Jnxcosifstatflagtable—jnxCosIfstatFlags and jnxCosIfIndex. Jnxcosqstattable—jnxCosQstatTxedPkts, jnxCosQstatTxedPktRate, jnxCosQstatTxedBytes, and jnxCosQstatTxedByteRate. Jnxcosfcidtable—jnxCosFcIdToFcName. Jnxcosfctable—jnxCosFcQueueNr. <p>The QFabric system does not support any traps for this MIB.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-cos.txt.</p> <p>For more information, see <i>Class-of-Service MIB</i>.</p>

Table 15: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems (*continued*)

MIB	Description
Configuration Management MIB (mib-jnx-cfgmgmt)	<p>Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made.</p> <p>A history of the last 32 configuration changes is kept in jnxCmChgEventTable.</p> <p>NOTE: On the QFabric system, these conditions apply:</p> <ul style="list-style-type: none"> • All scalar variables under the jnxCmCfgChg table are supported. • Supported scalar OIDs are jnxCmCfgChgLatestIndex, jnxCmCfgChgLatestTime, jnxCmCfgChgLatestDate, jnxCmCfgChgLatestSource, jnxCmCfgChgLatestUser, and jnxCmCfgChgMaxEventEntries. • Scalar variables under the jnxCmRescueChg table are not supported. <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-cfgmgmt.txt.</p> <p>For more information, see <i>Configuration Management MIB</i>.</p>
Fabric Chassis MIB (mib-jnx-fabric-chassis)	<p>Provides hardware information about the QFabric system and its component devices. This MIB is based on the Juniper Networks enterprise-specific Chassis MIB but adds another level of indexing that provides information for QFabric system component devices.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-fabric-chassis.txt.</p> <p>For more information, see “Fabric Chassis MIB” on page 44.</p>
Interface MIB (Extensions) (mib-jnx-if-extensions)	<p>Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables.</p> <p>NOTE: On the QFabric system, scalar variables are not supported.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-if-extensions.txt.</p> <p>For more information, see <i>Interface MIB</i>.</p>
Power Supply Unit MIB (mib-jnx-power-supply-unit)	<p>Provides support for environmental monitoring of the power supply unit for the Interconnect device of the QFabric system.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-power-supply-unit.txt.</p> <p>For more information, see <i>Power Supply Unit MIB</i>.</p> <p>NOTE: On the QFabric system, scalar variables for the jnxPsuObjects 1 object ID in the jnxPsuScalars table are not supported.</p>

Table 15: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems (*continued*)

MIB	Description
QFabric MIB (jnx-qf-smi)	<p>Explains how the Juniper Networks enterprise-specific QFabric MIBs are structured. Defines the MIB objects that are reported by the QFabric system and the contents of the traps that can be issued by the QFabric system.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-qf-smi.txt.</p>
Utility MIB (mib-jnx-util)	<p>Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.</p> <p>For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos13.2/topics/reference/mibs/mib-jnx-util.txt.</p> <p>For more information, see “Utility MIB” on page 48 and “Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage” on page 186.</p>

Related Documentation

- *SNMP MIBs and Traps Reference*
- [Understanding the Implementation of SNMP on page 39](#)
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
- [SNMP Traps Support on page 72](#)

SNMP Traps Support

The QFX Series standalone switches, QFX Series Virtual Chassis, QFabric systems, and OCX Series support standard SNMP traps and Juniper Networks enterprise-specific traps.

For more information, see:

- [SNMP Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series on page 72](#)
- [SNMP Traps Supported on QFabric Systems on page 81](#)

SNMP Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

QFX Series standalone switches, QFX Series Virtual Chassis, and OCX Series support SNMPv1 and v2 traps. For more information, see:

- [SNMPv1 Traps on page 73](#)
- [SNMPv2 Traps on page 77](#)

SNMPv1 Traps

QFX Series standalone switches, QFX Series Virtual Chassis, and OCX Series support both standard SNMPv1 traps and Juniper Networks enterprise-specific SNMPv1 traps. See:

- [Table 16 on page 73](#) for standard SNMPv1 traps.
- [Table 17 on page 75](#) for enterprise-specific SNMPv1 traps.

The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

Table 16: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
Link Notifications						
RFC 1215, <i>Conventions for Defining Traps for Use with the SNMP</i>	linkDown	1.3.6.1.4.1.2636	2	0	Warning	SNMP_TRAP_LINK_DOWN
	linkUp	1.3.6.1.4.1.2636	3	0	Info	SNMP_TRAP_LINK_UP
Remote Operations Notifications						
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i>	pingProbeFailed	1.3.6.1.2.1.80.0	6	1	Info	SNMP_TRAP_PING_PROBE_FAILED
	pingTestFailed	1.3.6.1.2.1.80.0	6	2	Info	SNMP_TRAP_PING_TEST_FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0	6	3	Info	SNMP_TRAP_PING_TEST_COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0	6	1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE
	traceRouteTestFailed	1.3.6.1.2.1.81.0	6	2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0	6	3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED
RMON Alarms						

Table 16: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
RFC 2819a, <i>RMON MIB</i>	fallingAlarm	1.3.6.1.2.1.16	6	2	–	–
	risingAlarm	1.3.6.1.2.1.16	6	1	–	–
Routing Notifications						
<i>BGP 4 MIB</i>	bgpEstablished	1.3.6.1.2.1.15.7	6	1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7	6	2	–	–
<i>OSPF TRAP MIB</i>	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2	6	1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2	6	2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2	6	3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2	6	4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2	6	5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2	6	6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2	6	7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2	6	10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2	6	11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2	6	13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2	6	16	–	–
Startup Notifications						
RFC 1215, <i>Conventions for Defining Traps for Use with the SNMP</i>	authenticationFailure	1.3.6.1.4.1.2636	4	0	Notice	SNMPD_TRAP_GEN_FAILURE
	coldStart	1.3.6.1.4.1.2636	0	0	Critical	SNMPD_TRAP_COLD_START

Table 16: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
	warmStart	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_WARM_START
VRRP Notifications						
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i>	vrrpTrapNewMaster	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW_MASTER_TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_FAILURE_TRAP

Table 17: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
Chassis Notifications (Alarm Conditions)						
<i>Chassis MIB</i> (jnx-chassis.mib)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1	6	1	Warning	CHASSISD_SNMP_TRAP
	jnxFanFailure	1.3.6.1.4.1.2636.4.1	6	2	Critical	CHASSISD_SNMP_TRAP
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1	6	3	Alert	CHASSISD_SNMP_TRAP
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Notice	CHASSISD_SNMP_TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Notice	CHASSISD_SNMP_TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1	6	7	Notice	CHASSISD_SNMP_TRAP
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1	6	8	Notice	CHASSISD_SNMP_TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1	6	9	Warning	CHASSISD_SNMP_TRAP

Table 17: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
	jnxFruOffline	1.3.6.1.4.1.2636.4.1	6	10	Notice	CHASSISD_SNMP_TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1	6	11	Notice	CHASSISD_SNMP_TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1	6	12	Warning	CHASSISD_SNMP_TRAP
	jnxPowerSupplyOk	1.3.6.1.4.1.2636.4.2	6	1	Critical	CHASSISD_SNMP_TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2	6	2	Critical	CHASSISD_SNMP_TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2	6	3	Alert	CHASSISD_SNMP_TRAP
Configuration Notifications						
<i>Configuration Management MIB</i> (jnx-configmgmt.mib)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5	6	1	—	—
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5	6	2	—	—
Remote Operations						
<i>Ping MIB</i> (jnx-ping.mib)	jnxPingRttThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	1	—	—
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	2	—	—
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	3	—	—
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	4	—	—
	jnxPingEgressStdDev ThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	5	—	—
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	6	—	—
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	7	—	—

Table 17: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	9	–	–
RMON Alarms						
<i>RMON MIB</i> (jnx-rmon. mib)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4.3	6	1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3	6	2	–	–

SNMPv2 Traps

- [Table 18 on page 77](#) lists the standard SNMP traps
- [Table 19 on page 79](#) lists the Juniper Networks enterprise-specific traps

Table 18: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, <i>The Interfaces Group MIB</i>	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_LINK_UP
Remote Operations Notifications				
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i>	pingProbeFailed	1.3.6.1.2.1.80.0.1	Info	SNMP_TRAP_PING_PROBE_FAILED
	pingTestFailed	1.3.6.1.2.1.80.0.2	Info	SNMP_TRAP_PING_TEST_FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Info	SNMP_TRAP_PING_TEST_COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE

Table 18: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED
RMON Alarms				
RFC 2819a, <i>RMON MIB</i>	fallingAlarm	1.3.6.1.2.1.16.0.1	–	–
	risingAlarm	1.3.6.1.2.1.16.0.2	–	–
Routing Notifications				
<i>BGP 4 MIB</i>	bgpEstablished	1.3.6.1.2.1.15.7.1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7.2	–	–
<i>OSPF Trap MIB</i>	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	–	–

Table 18: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Startup Notifications				
RFC 1907, <i>Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_GEN_FAILURE
VRRP Notifications				
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i>	vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1	Warning	VRRPD_NEWMASTER_TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	Warning	VRRPD_AUTH_FAILURE_TRAP

Table 19: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Chassis (Alarm Conditions) Notifications				
<i>Chassis MIB</i> (mib-jnx-chassis)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1.1	Alert	CHASSISD_SNMP_TRAP
	jnxFanFailure	1.3.6.1.4.1.2636.4.1.2	Critical	CHASSISD_SNMP_TRAP
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1.3	Critical	CHASSISD_SNMP_TRAP
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1.5	Notice	CHASSISD_SNMP_TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1.6	Notice	CHASSISD_SNMP_TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1.7	Notice	CHASSISD_SNMP_TRAP

Table 19: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1.8	Notice	CHASSISD_SNMP_TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1.9	Warning	CHASSISD_SNMP_TRAP
	jnxFruOffline	1.3.6.1.4.1.2636.4.1.10	Notice	CHASSISD_SNMP_TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1.11	Notice	CHASSISD_SNMP_TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1.12	Notice	CHASSISD_SNMP_TRAP
	jnxPowerSupplyOK	1.3.6.1.4.1.2636.4.2.1	Critical	CHASSISD_SNMP_TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2.2	Critical	CHASSISD_SNMP_TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2.3	Alert	CHASSISD_SNMP_TRAP
Configuration Notifications				
<i>Configuration Management MIB</i> (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				

Table 19: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches, QFX Series Virtual Chassis, and OCX Series (*continued*)

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
<i>Ping MIB</i> (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–
RMON Alarms				
<i>RMON MIB</i> (mib-jnx-rmon)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4.3.0.1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3.0.2	–	–

SNMP Traps Supported on QFabric Systems

QFabric systems support standard SNMPv2 traps and Juniper Networks enterprise-specific SNMPv2 traps.



NOTE: QFabric systems do not support SNMPv1 traps.

For more information, see:

- [Table 20 on page 82](#) for standard SNMPv2 traps

- [Table 21 on page 83](#) for Juniper Networks enterprise-specific SNMPv2 traps

Table 20: Standard SNMPv2 Traps Supported on QFabric Systems

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, <i>The Interfaces Group MIB</i>	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_LINK_UP
Startup Notifications				
RFC 1907, <i>Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_GEN_FAILURE

Table 21: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
<i>Fabric Chassis MIB</i> (mib-jnx-fabric-chassis)	Fabric Chassis (Alarm Conditions) Notifications			
	jnxFabricPowerSupplyFailure	1.3.6.1.4.1.2636.4.19.1	Warning	–
	jnxFabricFanFailure	1.3.6.1.4.1.2636.4.19.2	Critical	–
	jnxFabricOverTemperature	1.3.6.1.4.1.2636.4.19.3	Alert	–
	jnxFabricRedundancySwitchover	1.3.6.1.4.1.2636.4.19.4	Notice	–
	jnxFabricFruRemoval	1.3.6.1.4.1.2636.4.19.5	Notice	–
	jnxFabricFruInsertion	1.3.6.1.4.1.2636.4.19.6	Notice	–
	jnxFabricFruPowerOff	1.3.6.1.4.1.2636.4.19.7	Notice	–
	jnxFabricFruPowerOn	1.3.6.1.4.1.2636.4.19.8	Notice	–
	jnxFabricFruFailed	1.3.6.1.4.1.2636.4.19.9	Warning	–
	jnxFabricFruOffline	1.3.6.1.4.1.2636.4.19.10	Notice	–
	jnxFabricFruOnline	1.3.6.1.4.1.2636.4.19.11	Notice	–
	jnxFabricFruCheck	1.3.6.1.4.1.2636.4.19.12	Warning	–
	jnxFabricFEBSwitchover	1.3.6.1.4.1.2636.4.19.13	Warning	–
	jnxFabricHardDiskFailed	1.3.6.1.4.1.2636.4.19.14	Warning	–
	jnxFabricHardDiskMissing	1.3.6.1.4.1.2636.4.19.15	Warning	–
	jnxFabricBootFromBackup	1.3.6.1.4.1.2636.4.19.16	Warning	–
	Fabric Chassis (Alarm Cleared Conditions) Notifications			
	jnxFabricPowerSupplyOK	1.3.6.1.4.1.2636.4.20.1	Critical	–
	jnxFabricFanOK	1.3.6.1.4.1.2636.4.20.2	Critical	–
	jnxFabricTemperatureOK	1.3.6.1.4.1.2636.4.20.3	Alert	–
	jnxFabricFruOK	1.3.6.1.4.1.2636.4.20.4	–	–

Table 21: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems (*continued*)

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
<i>QFabric MIB</i> (mib-jnx-qf-smi)	QFabric MIB Notifications			
	jnxQFabricDownloadIssued	1.3.6.1.4.1.2636.3.42.1.0.1	–	–
	jnxQFabricDownloadFailed	1.3.6.1.4.1.2636.3.42.1.0.2	–	–
	jnxQFabricDownloadSucceeded	1.3.6.1.4.1.2636.3.42.1.0.3	–	–
	jnxQFabricUpgradeIssued	1.3.6.1.4.1.2636.3.42.1.0.4	–	–
	jnxQFabricUpgradeFailed	1.3.6.1.4.1.2636.3.42.1.0.5	–	–
	jnxQFabricUpgradeSucceeded	1.3.6.1.4.1.2636.3.42.1.0.6	–	–
Configuration Notifications				
<i>Configuration Management MIB</i> (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				
<i>Ping MIB</i> (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–

- Related Documentation**
- [SNMP MIBs and Traps Reference](#)
 - [Understanding the Implementation of SNMP on page 39](#)
 - [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
 - [SNMP MIBs Support on page 56](#)

MIB Objects for the QFX Series

This topic lists the Juniper Networks enterprise-specific SNMP Chassis MIB definition objects for the QFX Series:

- [QFX Series Standalone Switches on page 85](#)
- [QFabric Systems on page 85](#)
- [QFabric System QFX3100 Director Device on page 86](#)
- [QFabric System QFX3008-I Interconnect Device on page 86](#)
- [QFabric System QFX3600-I Interconnect Device on page 86](#)
- [QFabric System Node Devices on page 87](#)

QFX Series Standalone Switches

```
jnxProductLineQFXSwitch      OBJECT IDENTIFIER ::= { jnxProductLine      82 }
jnxProductNameQFXSwitch      OBJECT IDENTIFIER ::= { jnxProductName      82 }
jnxProductModelQFXSwitch     OBJECT IDENTIFIER ::= { jnxProductModel     82 }
jnxProductVariationQFXSwitch OBJECT IDENTIFIER ::= { jnxProductVariation 82 }
jnxProductQFX3500s          OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 1 }
jnxProductQFX360016QS       OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 2 }
jnxProductQFX350048T4QS     OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 3 }
jnxProductQFX510024Q        OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 4 }
jnxProductQFX510048S6Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 5 }

jnxChassisQFXSwitch          OBJECT IDENTIFIER ::= { jnxChassis          82 }

jnxSlotQFXSwitch             OBJECT IDENTIFIER ::= { jnxSlot             82 }
jnxQFXSwitchSlotFPC          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch      1 }
jnxQFXSwitchSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch      2 }
jnxQFXSwitchSlotPower        OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch      3 }
jnxQFXSwitchSlotFan          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch      4 }
jnxQFXSwitchSlotFPB          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch      5 }

jnxMediaCardSpaceQFXSwitch   OBJECT IDENTIFIER ::= { jnxMediaCardSpace 82 }
jnxQFXSwitchMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXSwitch 1 }
```

QFabric Systems

```
jnxProductLineQFX3000      OBJECT IDENTIFIER ::= { jnxProductLine 84 }
jnxProductNameQFX3000      OBJECT IDENTIFIER ::= { jnxProductName 84 }
jnxProductModelQFX3000     OBJECT IDENTIFIER ::= { jnxProductModel 84 }
jnxProductVariationQFX3000 OBJECT IDENTIFIER ::= { jnxProductVariation 84 }
jnxProductQFX3000-G        OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 1 }
jnxProductQFX3000-M        OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 2 }
jnxChassisQFX3000          OBJECT IDENTIFIER ::= { jnxChassis      84 }
```


QFabric System QFX3100 Director Device

```
jnxProductLineQFX3100 OBJECT IDENTIFIER ::= { jnxProductLine      100 }
jnxProductNameQFX3100 OBJECT IDENTIFIER ::= { jnxProductName      100 }
jnxProductModelQFX3100 OBJECT IDENTIFIER ::= { jnxProductModel    100 }
jnxProductVariationQFX3100 OBJECT IDENTIFIER ::= { jnxProductVariation 100 }
jnxChassisQFX3100      OBJECT IDENTIFIER ::= { jnxChassis         100 }

jnxSlotQFX3100          OBJECT IDENTIFIER ::= { jnxSlot           100 }
jnxQFX3100SlotCPU       OBJECT IDENTIFIER ::= { jnxSlotQFX3100    1 }
jnxQFX3100SlotMemory    OBJECT IDENTIFIER ::= { jnxSlotQFX3100    2 }
jnxQFX3100SlotPower     OBJECT IDENTIFIER ::= { jnxSlotQFX3100    3 }
jnxQFX3100SlotFan       OBJECT IDENTIFIER ::= { jnxSlotQFX3100    4 }
jnxQFX3100SlotHardDisk  OBJECT IDENTIFIER ::= { jnxSlotQFX3100    5 }
jnxQFX3100SlotNIC       OBJECT IDENTIFIER ::= { jnxSlotQFX3100    6 }
```

QFabric System QFX3008-I Interconnect Device

```
jnxProductLineQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      60 }
jnxProductNameQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductName      60 }
jnxProductModelQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductModel    60 }
jnxProductVariationQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductVariation 60 }
jnxProductQFX3008          OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 1 }
jnxProductQFXC083008       OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 2 }
jnxProductQFX3008I         OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 3 }

jnxChassisQFXInterconnect   OBJECT IDENTIFIER ::= { jnxChassis         60 }

jnxSlotQFXInterconnect      OBJECT IDENTIFIER ::= { jnxSlot           60 }
jnxQFXInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 1 }
jnxQFXInterconnectSlotHBM   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 2 }
jnxQFXInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 3 }
jnxQFXInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 4 }
jnxQFXInterconnectSlotCBD   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 5 }
jnxQFXInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect 6 }

jnxMediaCardSpaceQFXInterconnect OBJECT IDENTIFIER ::= { jnxMediaCardSpace 60 }
jnxQFXInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXInterconnect 1 }

jnxMidplaneQFXInterconnect  OBJECT IDENTIFIER ::= { jnxBackplane        60 }
```

QFabric System QFX3600-I Interconnect Device

```
jnxProductLineQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      91 }
jnxProductNameQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductName      91 }
jnxProductModelQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductModel    91 }
jnxProductVariationQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductVariation 91 }
jnxProductQFX3600I         OBJECT IDENTIFIER ::= { jnxProductVariationQFXMInterconnect 1 }

jnxChassisQFXMInterconnect   OBJECT IDENTIFIER ::= { jnxChassis         91 }

jnxSlotQFXMInterconnect      OBJECT IDENTIFIER ::= { jnxSlot           91 }
jnxQFXMInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect 1 }
jnxQFXMInterconnectSlotHBM   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect 2 }
jnxQFXMInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect 3 }
jnxQFXMInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect 4 }
jnxQFXMInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect 5 }
```



```
jnxMediaCardSpaceQFXMInterconnect OBJECT IDENTIFIER ::= { jnxMediaCardSpace 91 }
jnxQFXMInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXMInterconnect 1 }
```

QFabric System Node Devices

```
jnxProductLineQFXNode OBJECT IDENTIFIER ::= { jnxProductLine 61 }
jnxProductNameQFXNode OBJECT IDENTIFIER ::= { jnxProductName 61 }
jnxProductModelQFXNode OBJECT IDENTIFIER ::= { jnxProductModel 61 }
jnxProductVariationQFXNode OBJECT IDENTIFIER ::= { jnxProductVariation 61 }
jnxProductQFX3500 OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 1 }
jnxProductQFX360016Q OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 3 }

jnxChassisQFXNode OBJECT IDENTIFIER ::= { jnxChassis 61 }

jnxSlotQFXNode OBJECT IDENTIFIER ::= { jnxSlot 61 }
jnxQFXNodeSlotFPC OBJECT IDENTIFIER ::= { jnxSlotQFXNode 1 }
jnxQFXNodeSlotHM OBJECT IDENTIFIER ::= { jnxSlotQFXNode 2 }
jnxQFXNodeSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXNode 3 }
jnxQFXNodeSlotFan OBJECT IDENTIFIER ::= { jnxSlotQFXNode 4 }
jnxQFXNodeSlotFPB OBJECT IDENTIFIER ::= { jnxSlotQFXNode 5 }

jnxMediaCardSpaceQFXNode OBJECT IDENTIFIER ::= { jnxMediaCardSpace 61 }
jnxQFXNodeMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXNode 1 }
```

- Related Documentation**
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
 - [Fabric Chassis MIB on page 44](#)

CHAPTER 7

System Logging

- [Overview of Junos OS System Log Messages on page 89](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)
- [Understanding the Implementation of System Log Messages on the QFabric System on page 91](#)

Overview of Junos OS System Log Messages

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the switch, including the following:

- Routine operations, such as a user login into the configuration database.
- Failure and error conditions, such as failure to access a configuration file.
- Emergency or critical conditions, such as power-down of the switch due to excessive temperature.

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the *Junos OS System Log Messages Reference*.



.....

NOTE: OCX Series switches comprise both the Junos OS and the host operating system (OS). For information about system logging on the host OS, see *Managing Host OS System Log and Core Files*.

.....

Related Documentation

- [Junos OS System Log Configuration Statements on page 144](#)
- [Junos OS Minimum System Logging Configuration on page 144](#)

Overview of Single-Chassis System Logging Configuration

The Junos OS system logging utility on the QFX Series and OCX Series is similar to the UNIX **syslogd** utility. This topic describes how to configure system logging for a single-chassis system that runs the Junos OS.

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions. You always specify the facility and severity of the messages to include in the log. For more information, see *Specifying the Facility and Severity of Messages to Include in the Log*.

You direct messages to one or more destinations by including the appropriate statement at the `[edit system syslog]` hierarchy level:

- To a named file in a local file system, by including the **file** statement. See [“Directing System Log Messages to a Log File” on page 146](#).
- To the terminal session of one or more specific users (or all users) when they are logged in to the switch, by including the **user** statement. See [“Directing System Log Messages to a User Terminal” on page 147](#).
- To the switch console, by including the **console** statement. See [“Directing System Log Messages to the Console” on page 148](#).
- To a remote machine that is running the **syslogd** utility, by including the **host** statement. See [“Directing System Log Messages to a Remote Machine” on page 147](#).

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the *Junos OS System Log Messages Reference*. You can alter the content and format of logged messages in the following ways:

- You can log messages to a file in structured-data format instead of the standard Junos OS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see [“Logging Messages in Structured-Data Format” on page 152](#).
- A message’s facility and severity level are together referred to as its *priority*. By default, the standard Junos OS format for messages does not include priority information (structured-data format includes a priority code by default). To include priority information in standard-format messages directed to a file or a remote destination, include the **explicit-priority** statement. For more information, see [“Including Priority Information in System Log Messages” on page 150](#).
- By default, the standard Junos OS format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see [“Including the Year or Millisecond in Timestamps” on page 151](#).
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by Junos OS or messages generated on

particular switches. For more information, see [“Directing System Log Messages to a Remote Machine” on page 147](#).

- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination. For more information, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 164](#).



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

Related Documentation

- [Examples: Configuring System Logging on page 166](#)
- [Specifying the Facility and Severity of Messages to Include in the Log](#)
- [Junos OS System Logging Facilities and Message Severity Levels on page 159](#)
- [Directing System Log Messages to a Log File on page 146](#)
- [Directing System Log Messages to a Remote Machine on page 147](#)
- [Directing System Log Messages to a User Terminal on page 147](#)
- [Directing System Log Messages to the Console on page 148](#)

Understanding the Implementation of System Log Messages on the QFabric System

This topic provides an overview of system log (syslog) messages as implemented on the QFabric system.

The QFabric system monitors events that occur on its component devices and distributes system log messages about those events to all external system log message servers (hosts) that are configured. Component devices may include Node devices, Interconnect devices, Director devices, and the Virtual Chassis. Messages are stored for viewing only in the QFabric system database. To view the messages, issue the **show log** command.

You configure system log messages by using the **host** and **file** statements at the **[edit system syslog]** hierarchy level. Use the **show log filename** operational mode command to view the messages.



NOTE: On the QFabric system, a syslog file named `messages` with a size of 100 MB is configured by default. If you do not configure a filename, you can use the default filename `messages` with the `show log filename` command.

All messages with a severity level of notice or higher are logged. Messages with a facility level of interactive-commands on Node devices are not logged.

The QFabric system supports the following system log message features:

- The **file *filename*** and **host *hostname*** statements at the **[edit system syslog]** hierarchy level are supported. Other statements at that hierarchy level are not supported.
- You can specify the maximum amount of data that is displayed when you issue the **show log *filename*** command by configuring the **file *filename* archive *maximum-file-size*** statement.
- You can specify that one or more system log message servers receive messages, which are sent to each server that is configured.
- If you configured an alias for a device or interface, the alias is displayed in the message for the device or interface.
- The level of detail that is included in a message depends on the facility and severity levels that are configured. Messages include the highest level of detail available for the configured facility and severity levels.
- The unit of time is measured and displayed in seconds, and not milliseconds. If you attempt to configure the **time-format** option in milliseconds, the log output displays **000**.

Starting in Junos OS Release 13.1, the QFabric system supports these additional syslog features:

- You can filter the output of the **show log *filename*** operational mode command by device type and device ID or device alias when you specify the **device-type (*device-id* | *device-alias*)** optional parameters. Device types include **director-device**, **infrastructure-device**, **interconnect-device**, and **node-device**.
- You can specify the syslog structured data output format when you configure the **structured-data** statement at the **[edit system syslog file *filename*]** and **[edit system syslog host *hostname*]** hierarchy levels.



NOTE: Information displayed in the structured data output for system logs originating from the Director software may not be complete.

- You can filter the types of logs that the Director group collects from a component device when you configure the **filter all *facility severity*** or **filter all match "*regular-expression*"** statements at the **[edit system syslog]** hierarchy level.

Unsupported syslog features include:

- File access to syslog messages
- Monitoring of syslog messages

**Related
Documentation**

- [Example: Configuring System Log Messages on page 169](#)
- [syslog \(QFabric System\) on page 375](#)

PART 2

Configuring

- [Network Management on page 95](#)
- [Automation Scripts on page 99](#)
- [Fabric OAM on page 103](#)
- [sFlow Technology on page 115](#)
- [SNMP on page 121](#)
- [System Log Messages on page 143](#)

CHAPTER 8

Network Management

- [Configuring Console and Auxiliary Port Properties on page 95](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 96](#)
- [Configuring Telnet Service for Remote Access to a Switch on page 98](#)

Configuring Console and Auxiliary Port Properties

The console port and auxiliary port on a switch provide out-of-band remote access to the switch. You can configure the console and auxiliary ports so that an external data terminal may be connected to the switch. The console port is enabled by default. The console port speed is 9600 baud, except on OCX Series devices, on which it is 115200 baud. The auxiliary port is disabled by default.

By default, terminal connections to the console and auxiliary ports are secure. When you configure the console and auxiliary ports as insecure, root logins are not allowed to establish terminal connections, and superusers and anyone with a user identifier (UID) of 0 are not allowed to establish terminal connections in multiuser mode.

To configure the console and auxiliary port properties on the switch:

1. To specify that the console port session should terminate if the connection to the data carrier is lost:

```
[edit system ports]
user@switch# set console log-out-on-disconnect
```

2. To specify the auxiliary port terminal type:

```
[edit system ports]
user@switch# set auxiliary type (ansi | small-xterm | vt100 | xterm)
```

For example, to specify the auxiliary port terminal type of **xterm** with a display of 80 columns by 65 rows:

```
[edit system ports]
user@switch# set auxiliary type xterm
```

3. To check the configuration:

```
[edit system ports]
user@switch# show
console log-out-on-disconnect;
auxiliary type xterm;
```


- Related Documentation**
- *auxiliary*
 - *console (Physical Port)*
 - *ports*

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch to accept SSH as an access service, include the **ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ssh {
  ciphers [ cipher-1 cipher-2 cipher-3 ... ]
  client-alive-count-max number;
  client-alive-interval seconds;
  connection-limit limit;
  hostkey-algorithm <algorithm | no-algorithm>;
  key-exchange algorithm;
  macs algorithm;
  max-sessions-per-connection number;
  no-passwords;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login <allow | deny | deny-password>;
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **max-sessions-per-connection *number***—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit the number of cloned sessions tunneled within a single SSH connection. The default value is 10.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router. Use the **no-tcp-forwarding** option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

- [Configuring the Root Login Through SSH on page 97](#)
- [Configuring the SSH Protocol Version on page 97](#)
- [Configuring the Client Alive Mechanism on page 97](#)

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH. To control user access through SSH, include the **root-login** statement at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router or switch as root through SSH. The default is **allow**.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

Configuring the SSH Protocol Version

By default, both version 1 and version 2 of the SSH protocol are enabled. To configure the router or switch to use only version 1 of the SSH protocol, include the **protocol-version** statement and specify **v1** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 ];
```

To configure the router or switch to use only version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

To explicitly configure the router or switch to use version 1 and 2 of the SSH protocol, include the **protocol-version** statement and specify **v1** and **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 v2 ];
```

For J Series Services Routers, the export license software supports SSH version 1 only.

Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the

client-alive-count-max and the **client-alive-interval**. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

Configuring Telnet Service for Remote Access to a Switch

Telnet provides unencrypted access to network devices. Configuring Telnet service for a switch enables in-band remote access to the switch.

By default, the switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute. Optionally, you can change the default Telnet settings by configuring the connection limit and rate limit at the **[edit system services telnet]** hierarchy level.

The connection limit is the maximum number of simultaneous connections per protocol (IPv4). The range is from 1 through 250. The default is 75.

The rate limit is the maximum number of connection attempts accepted per minute per protocol. The range is from 1 through 250. The default is 150.

To configure Telnet service:

1. To specify the connection limit:

```
[edit system services]
user@switch# set telnet connection-limit connection-limit
```

2. To specify the rate limit:

```
[edit system services]
user@switch# set telnet rate-limit rate-limit
```

3. Check that the Telnet connection limit and rate limit show the values you specified:

```
[edit system services]
user@switch# show
telnet {
  connection-limit 50;
  rate-limit 100;
}
```

Related Documentation

- [Understanding Telnet on the QFabric System on page 7](#)
- *Limiting the Number of User Login Attempts for SSH and Telnet Sessions*
- *Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions*

CHAPTER 9

Automation Scripts

- [Controlling the Execution of Commit Scripts on page 99](#)

Controlling the Execution of Commit Scripts

This document describes the tasks that affect the way commit scripts are executed. In the QFabric system, commit scripts are stored in the in the `/pbdata/mgd_shared/partition-ip/var/db/scripts/commit` directory that is shared among Director devices in a Director group.

To determine which commit scripts are currently enabled on the QFabric system, use the **show** command to display the files included at the `[edit system scripts commit]` hierarchy level. To ensure that the enabled files are on the device, list the contents of the `/pbdata/mgd_shared/partition-ip/var/db/scripts/commit` directory using the **file list** operational mode command.

See the following tasks:

- [Enabling Commit Scripts to Execute on page 99](#)
- [Removing Commit Scripts from the Configuration on page 100](#)
- [Deactivating Commit Scripts on page 101](#)
- [Activating Inactive Commit Scripts on page 101](#)

Enabling Commit Scripts to Execute

The commit operation requires that all scripts be included in configuration at the `[edit system scripts commit file]` hierarchy level for all QFabric Director devices.

If you need to temporarily remove a script from a commit operation but do not want to remove it from the configuration permanently, you may configure the **optional** statement at the `[edit system scripts commit file filename]` hierarchy level to enable the commit operation to succeed even if a script is missing from the commit script directory.



CAUTION: When you include the **optional** statement at the `[edit system scripts commit file filename]` hierarchy level, no error message is generated during the commit operation if the file does not exist. As a result, you might not be aware that a script has not been executed as expected.

The filename of a commit script written in SLAX must include the **.slax** extension for the script to be executed.

To enable a commit script to execute during a commit operation:

1. Ensure that the commit script is located in the correct directory:
/pbdata/mgd_shared/partition-ip/var/db/scripts/commit directory on the Director device.

2. Configure the commit script.

```
[edit system scripts commit]
user@switch# set file filename <optional>
```

3. Commit the configuration.

```
[edit system scripts commit]
user@switch# top
[edit]
user@switch# commit
```

Removing Commit Scripts from the Configuration

You can prevent commit scripts from executing during a commit operation by removing the scripts from the commit directory in the configuration.



NOTE: You can also deactivate a script using the **deactivate** statement instead of removing it from the configuration. Deactivated scripts may be reactivated later.

To prevent a commit script from executing during a commit operation:

1. Delete the commit script file from the commit directory in the configuration.

```
[edit system scripts commit]
user@switch# delete file filename
```

2. Commit the configuration.

```
[edit system scripts commit]
user@switch# top
[edit]
user@switch# commit
```

3. Remove the commit script from the **/pbdata/mgd_shared/** directory on the Director device.



BEST PRACTICE: Although removing the commit script is not necessary, we recommend deleting unused files from the system.

Deactivating Commit Scripts

Deactivating a commit script results in its being marked as inactive in the configuration. The script is not executed during the commit operation, but you can reactivate the script by using the **activate** statement.

To deactivate the commit script:

1. Deactivate the script.

```
[edit]  
user@switch deactivate system scripts commit file filename
```

2. Commit your changes.

```
[edit]  
user@switch# commit
```

3. Verify that the commit script is deactivated.

```
[edit]  
user@switch# show system scripts commit  
inactive: file mycommit.slax
```

Activating Inactive Commit Scripts

Deactivating a commit script results in its being marked as inactive in the configuration and is therefore not executed during the commit operation.

To activate an inactive commit script:

1. Activate the script.

```
[edit]  
user@switch# activate system scripts commit file filename
```

2. Commit your changes.

```
[edit]  
user@switch# commit
```


CHAPTER 10

Fabric OAM

- [Configuring a Fabric Maintenance Association on page 103](#)
- [Configuring Flow Specifications on page 104](#)
- [Example: Configuring Internal Fabric OAM Monitoring on page 108](#)

Configuring a Fabric Maintenance Association

On a QFabric system, enabling internal fabric monitoring using the ping and traceroute operations requires that a fabric maintenance association (FMA) be configured in addition to a flow specification. The FMA associates a particular VLAN with a set of source and destination interfaces called fabric maintenance endpoints (FMEPs) that are used for tracing the flow path between the endpoints. Configuration of the VLAN name is mandatory.

Before configuring the FMA, configure a VLAN name (and not a VLAN ID) for the VLAN in which the internal fabric monitoring occurs. If you already configured a VLAN ID instead of a VLAN name, you must first delete the VLAN ID and then specify a VLAN name before you configure the FMA.



NOTE: Because each FMA and VLAN have a one-to-one correspondence, an FMA in each QFabric system must be given a unique name.

To configure an FMA:

1. Configure an FMA name that is unique within the QFabric system:

```
[edit protocols oam fabric]  
user@host# set fabric-maintenance-associations fma-name
```

2. (Optional) Configure the FMA description:

```
[edit protocols oam fabric]  
user@host# set fabric-maintenance-associations fma-name description string
```

3. Configure the VLAN name:

```
[edit protocols oam fabric]  
user@host# set fabric-maintenance-associations fma-name vlan-name vlan-name
```

4. Configure an FMEP, including the identifier, name, description, and associated interface:


```
[edit protocols oam fabric]
user@host# set fabric-maintenance-associations fma-name
fabric-maintenance-end-points fmeop-id fmeop-name name description string
fmeop-interface interface-name
```

5. Repeat Step 4 to configure additional FMEPs.

**Related
Documentation**

- [Overview of Internal Fabric Monitoring on page 29](#)
- [Configuring Flow Specifications on page 104](#)
- [fabric \(OAM\) on page 237](#)
- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

Configuring Flow Specifications

On a QFabric system, enabling internal fabric monitoring using the ping and traceroute operations requires that a flow specification be configured in addition to a fabric maintenance association (FMA). A flow specification is used to determine the contents of the packet that is used for a particular operation. For example, an Ethernet type flow specification describes the contents of a pure Layer 2 packet, whereas an Ethernet IPv4 type flow specification describes an Ethernet IPv4 packet.



NOTE: In the flow specification configuration, some parameters are optional. If you do not configure the optional parameters, the system generates random values that are used as PDU contents.

In order to replicate actual traffic behavior, internal fabric monitoring requires that the following flow specification fields be filled with the same values as the traffic packets:

- Unicast Ethernet—Source MAC address, destination MAC address, Ethertype
- Unicast IPv4—Source IP address, destination IP address, source L4 port, destination L4 port, destination MAC address

The configuration for each flow specification type includes parameters specific to that particular type. Use one of the following procedures to configure the flow specification for your flow type:

- [Configuring a Unicast Ethernet Flow Specification on page 105](#)
- [Configuring a Unicast Ethernet IPv4 Flow Specification on page 106](#)
- [Configuring a Multicast IPv4 Flow Specification on page 107](#)
- [Configuring a Multicast VLAN Flood Flow Specification on page 107](#)

Configuring a Unicast Ethernet Flow Specification

This procedure describes how to configure a flow specification for a unicast Ethernet flow type. This configuration is applicable for the unicast ping and traceroute operations.



NOTE: Some parameters are optional. If you do not configure the optional parameters, the system generates random values that are used as PDU contents.

In order to replicate actual traffic behavior, internal fabric monitoring requires that the following flow specification fields be filled with the same values as the traffic packets: source MAC address, destination MAC address, and Ethertype.

To configure a unicast Ethernet flow specification:

1. Configure a flow specification name:

```
[edit protocols oam fabric]
user@host# set flow-specs flow-specification-name
```

2. (Optional) Set the Ethernet frame size:

```
[edit protocols oam fabric]
user@host# set ethernet-frame-size ethernet-frame-size
```

3. Set the flow specification type as unicast Ethernet and specify the EtherType:

```
[edit protocols oam fabric flow-specs flow-specification-name]
user@host# set unicast-ethernet ethertype ethertype
```

4. (Optional) Set the MAC address and the MAC address range of the source FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet]
user@host# set source-mac source-mac-address source-mac-mask source-mac-mask
```



NOTE: Configuration of the source-mac and source-mac-mask parameters is optional, but the source-mac-mask parameter can be specified only if the source-mac parameter is also configured.

5. (Optional) Set the MAC address or address range mask for the destination FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet]
user@host# set destination-mac destination-mac-address destination-mac-mask destination-mac-mask
```



NOTE: Configuration of the destination-mac and destination-mac-mask parameters is optional, but the destination-mac-mask parameter can be specified only if the destination-mac parameter is also configured.

Configuring a Unicast Ethernet IPv4 Flow Specification

This procedure describes how to configure a flow specification for a unicast Ethernet IPv4 flow type. This configuration is applicable for the unicast ping and traceroute operations.



NOTE: All parameters except the flow specification name are optional. If you do not configure the optional parameters, the system generates random values that are used as PDU contents.

In order to replicate actual traffic behavior, internal fabric monitoring requires that the following flow specification fields be filled with the same values as the traffic packets: source IP address, destination IP address, source L4 port, destination L4 port, destination MAC address.

To configure a unicast Ethernet IPv4 flow specification:

1. Configure a flow specification name:

```
[edit protocols oam fabric]
user@host# set flow-specs flow-specification-name
```

2. (Optional) Set the Ethernet frame size:

```
[edit protocols oam fabric flow-specs flow-specification-name]
user@host# set ethernet-frame-size size
```

3. Set the flow specification type as unicast Ethernet IPv4:

```
[edit protocols oam fabric flow-specs flow-specification-name]
user@host# set unicast-ethernet-ipv4
```

4. (Optional) Set the IPv4 address or the address range of the source FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# set source-ip source-ip-address
```

or

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# set source-ip-mask source-ip-mask
```

5. (Optional) Set the IPv4 address or the address range of the destination FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# set destination-ip destination-ip-address
```

or

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# set destination-ip-mask destination-ip-mask
```

6. (Optional) Set the IPv4 protocol type:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# ip-protocol protocol
```

7. (Optional) Set the L4 port (TCP or UDP port number) of the source FMEP:


```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# source-l4-port source-l4-port-number
```

8. (Optional) Set the L4 port of the destination FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name unicast-ethernet-ipv4]
user@host# destination-l4-port destination-l4-port-number
```

Configuring a Multicast IPv4 Flow Specification

This procedure describes how to configure a flow specification for a multicast IPv4 flow type.



NOTE: Some parameters are optional. If you do not configure the optional parameters, the system generates random values that are used as PDU contents.

To configure a multicast IPv4 flow specification:

1. Configure a flow specification name:

```
[edit protocols oam fabric]
user@host# set flow-specs flow-specification-name
```

2. Set the flow specification type as multicast IPv4:

```
[edit protocols oam fabric flow-specs flow-specification-name]
user@host# set multicast-ipv4
```

3. (Optional) Set the IPv4 address of the source FMEP:

```
[edit protocols oam fabric flow-specs flow-specification-name multicast-ipv4]
user@host# set source-ip ipv4-address
```

4. Set the IPv4 multicast group address:

```
[edit protocols oam fabric flow-specs flow-specification-name multicast-ipv4]
user@host# set dest-ip-multicast-group ipv4-mcast-address
```

Configuring a Multicast VLAN Flood Flow Specification

This procedure describes how to configure a flow specification for a multicast VLAN flood flow type.

To configure a multicast VLAN flood flow specification:

1. Configure a flow specification name:

```
[edit protocols oam fabric]
user@host# set flow-specs flow-specification-name
```

2. Set the flow specification type as multicast VLAN flood:

```
[edit protocols oam fabric flow-specs flow-specification-name]
user@host# set multicast-vlan-flood
```


- Related Documentation**
- [Overview of Internal Fabric Monitoring on page 29](#)
 - [Configuring a Fabric Maintenance Association on page 103](#)
 - [fabric \(OAM\) on page 237](#)
 - [ping fabric multicast-flow on page 398](#)
 - [ping fabric unicast-flow on page 400](#)
 - [traceroute fabric unicast-flow on page 446](#)

Example: Configuring Internal Fabric OAM Monitoring

This example shows how to configure the internal fabric Operation, Administration, Maintenance (OAM) monitoring feature on the QFabric system, including the fabric maintenance association (FMA) and flow specifications for unicast Ethernet traffic.

Internal fabric monitoring enables you to validate the flow path of protocol data units (PDUs) across a given VLAN on the QFabric system using the ping operation.

Internal fabric monitoring is useful for fault detection on the QFabric system. For example, if a PDU reaches a destination that is not part of the VLAN configuration, the ping operation displays the exception on the console at runtime.

- [Requirements on page 108](#)
- [Overview on page 109](#)
- [Configuration on page 110](#)
- [Verification on page 112](#)

Requirements

This example uses the following hardware and software components:

- One QFabric system with the following components:
 - A Director group (two Director devices)
 - Two QFabric system Interconnect devices
 - Node devices, including:
 - One Node device (Node-81) configured in a default network Node group (NNW-NG-0)
 - One Node device (Node-80) in an autogenerated server Node group (SNG-80)
 - Two Node devices (Node-83 and Node-84) configured in a redundant server Node group (RSNG-8384)
- Junos OS Release 12.2 or later

Before you configure the FMA, first configure a VLAN in which the internal fabric OAM monitoring occurs. You can usually configure a VLAN by specifying a VLAN ID or VLAN name. However, in the case of the VLAN used for internal fabric OAM monitoring, you

must specify a VLAN name (not a VLAN ID). The FMA configuration requires a VLAN name and not a VLAN ID.

If you have already configured a VLAN ID for the VLAN, you must delete the VLAN ID from the associated interfaces and then add a VLAN name.

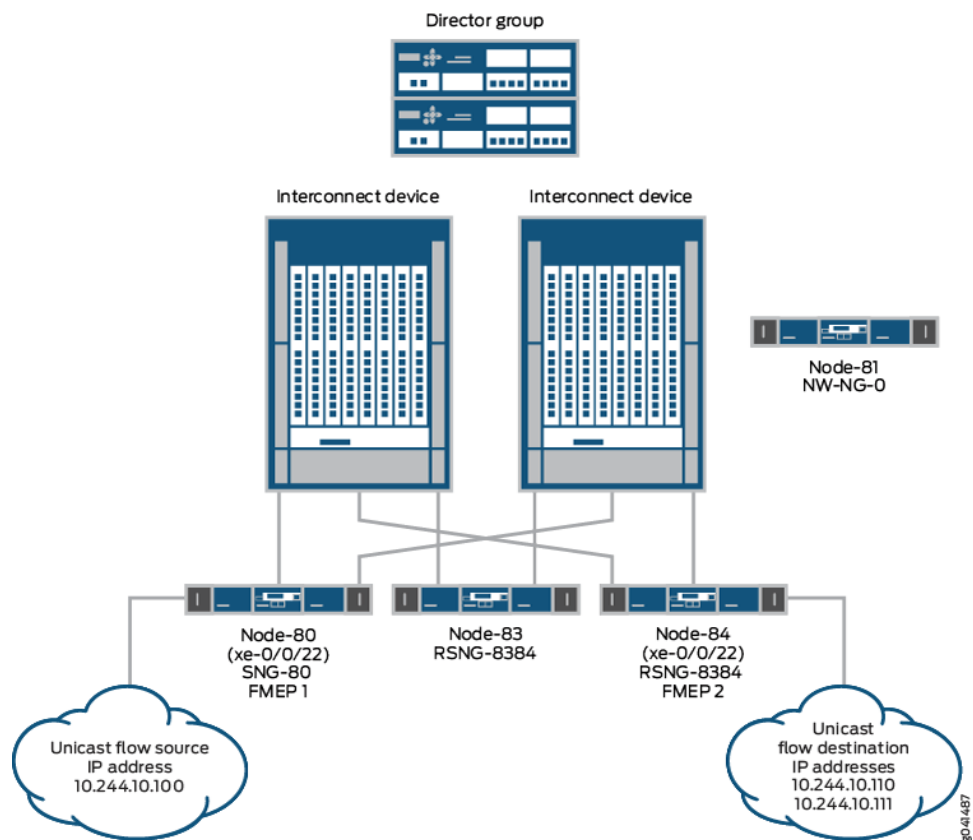
Overview

On a QFabric system, enabling internal fabric OAM monitoring requires that you configure an FMA and a flow specification.

- The *FMA* associates a particular VLAN with a set of source and destination interfaces called fabric maintenance endpoints (FMEPs) that are used for tracing the data path between the endpoints. Configuration of the VLAN name is mandatory when you configure an FMA.
- A *flow specification* is used to determine the contents of a packet that is used for a particular operation. For example, an Ethernet type flow specification describes the contents of a pure Layer 2 packet, whereas an Ethernet IPv4 type flow specification describes an Ethernet IPv4 packet.

Topology

This example uses the following topology:



- The QFabric system Node devices are connected to the Interconnect devices.
- Node device Node-80 is configured in the server Node group SNG-80.
- Node devices Node-83 and Node-84 are configured in a redundant server Node group RSNG-8384.
- The device with the unicast flow source IP address is connected to Node-80.
- The device with the unicast flow destination IP addresses is connected to Node-84.

Table 22 on page 110 maps the association of the fabric OAM elements configured in this example.

Table 22: Fabric OAM Configuration Elements

Interface	FMA	VLAN Name	FMEP ID	Flow Specifications
Node-80:xe-0/0/22	fma1	v10	1	<ul style="list-style-type: none"> flowspec1 flowspec2
Node-84:xe-0/0/22	fma1	v10	2	<ul style="list-style-type: none"> flowspec1 flowspec2

Configuration

CLI Quick Configuration

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

```

set vlans v10 vlan-id 10
set interfaces Node-80:xe-0/0/22 unit 0 family ethernet-switching vlan members v10
set interfaces Node-84:xe-0/0/22 unit 0 family ethernet-switching vlan members v10
set protocols oam fabric fabric-maintenance-associations fma1 vlan-name v10
set protocols oam fabric fabric-maintenance-associations fma1
    fabric-maintenance-end-points 1 fmep-interface Node-80:xe-0/0/22.0
set protocols oam fabric fabric-maintenance-associations fma1
    fabric-maintenance-end-points 2 fmep-interface Node-84:xe-0/0/22.0
set protocols oam fabric flow-specs flowspec1 unicast-ethernet-ipv4 source-ip
    10.244.10.100
set protocols oam fabric flow-specs flowspec1 unicast-ethernet-ipv4 destination-ip
    10.244.10.110
set protocols oam fabric flow-specs flowspec1 unicast-ethernet-ipv4 destination-mac
    00:00:80:8d:2d:15
set protocols oam fabric flow-specs flowspec1 unicast-ethernet-ipv4 source-l4-port 60
set protocols oam fabric flow-specs flowspec1 unicast-ethernet-ipv4 destination-l4-port
    80
set protocols oam fabric flow-specs flowspec2 unicast-ethernet-ipv4 source-ip
    10.244.10.100
set protocols oam fabric flow-specs flowspec2 unicast-ethernet-ipv4 destination-ip
    10.244.10.111
set protocols oam fabric flow-specs flowspec2 unicast-ethernet-ipv4 destination-mac
    00:00:80:8d:2d:17
set protocols oam fabric flow-specs flowspec2 unicast-ethernet-ipv4 source-l4-port 60

```



```
set protocols oam fabric flow-specs flowspec2 unicast-ethernet-ipv4 destination-l4-port
80
```

Step-by-Step Procedure

To configure internal fabric OAM monitoring:

1. Configure a name and ID for the VLAN.

```
[edit]
set vlans v10 vlan-id 10
```
2. Assign a set of interfaces to the VLAN.

```
[edit]
set interfaces Node-80:xe-0/0/22 unit 0 family ethernet-switching vlan members
v10
set interfaces Node-84:xe-0/0/22 unit 0 family ethernet-switching vlan members
v10
```
3. Define the FMA and associate it with a VLAN name.

```
[edit protocols oam fabric]
set fabric-maintenance-associations fma1 vlan-name v10
```
4. Configure FMEPs for the FMA.

```
[edit protocols oam fabric]
set fabric-maintenance-associations fma1 fabric-maintenance-end-points 1
fmeip-interface Node-80:xe-0/0/22.0
set fabric-maintenance-associations fma1 fabric-maintenance-end-points 2
fmeip-interface Node-84:xe-0/0/22.0
```
5. Configure two IPv4 flow specifications for unicast traffic from FMEP 1 to FMEP 2.

```
[edit protocols oam fabric]
set flow-specs flowspec1 unicast-ethernet-ipv4 source-ip 10.244.10.100
set flow-specs flowspec1 unicast-ethernet-ipv4 destination-ip 10.244.10.110
set flow-specs flowspec1 unicast-ethernet-ipv4 destination-mac 00:00:80:8d:2d:15
set flow-specs flowspec1 unicast-ethernet-ipv4 source-l4-port 60
set flow-specs flowspec1 unicast-ethernet-ipv4 destination-l4-port 80
set flow-specs flowspec2 unicast-ethernet-ipv4 source-ip 10.244.10.100
set flow-specs flowspec2 unicast-ethernet-ipv4 destination-ip 10.244.10.111
set flow-specs flowspec2 unicast-ethernet-ipv4 destination-mac 00:00:80:8d:2d:17
set flow-specs flowspec2 unicast-ethernet-ipv4 source-l4-port 60
set flow-specs flowspec2 unicast-ethernet-ipv4 destination-l4-port 80
```

Results Display the results of the configuration.

```
root@qfabric> show protocols oam fabric
fabric-maintenance-associations {
  fma1 {
    vlan-name v10;
    fabric-maintenance-end-points {
      1 {
        fmeip-interface Node-80:xe-0/0/22.0;
      }
      2 {
        fmeip-interface Node-84:xe-0/0/22.0;
      }
    }
  }
}
```



```

}
flow-specs {
  flowspec1 {
    unicast-ethernet-ipv4 {
      source-ip 10.244.10.100;
      destination-ip 10.244.10.110;
      destination-mac 0:0:80:8d:2d:15;
      source-l4-port 60;
      destination-l4-port 80;
    }
  }
  flowspec2 {
    unicast-ethernet-ipv4 {
      source-ip 10.244.10.100;
      destination-ip 10.244.10.111;
      destination-mac 0:0:80:8d:2d:17;
      source-l4-port 60;
      destination-l4-port 80;
    }
  }
}

```

Verification

Confirm that the configuration is working properly.

- [Verifying Configuration of Fabric OAM Interfaces on page 112](#)
- [Verifying Configuration of the Fabric OAM Flow Specification on page 113](#)
- [Verifying Operation of the Unicast ping Command on page 113](#)

Verifying Configuration of Fabric OAM Interfaces

Purpose Verify that the interfaces are associated with the FMA.

Action Display the fabric OAM interfaces.

root@qfabric> show oam fabric interfaces

Interface-name	Fabric-Maintenance Association	VLAN	Interface state	MEP Identifier	MEP Name
NW-NG-0:NULL	fma-default	*	up	32790	fmep-default-BBAK8793
NW-NG-0:NULL	fma-default	*	up	32791	fmep-default-BBAK8798
RSNG-8384:NULL	fma-default	*	up	32794	fmep-default-BBAK8748
RSNG-8384:NULL	fma-default	*	up	32795	fmep-default-BBAK0465
Node-84:xe-0/0/22.0	fma1	V10	up	2	
SNG-60:NULL	fma-default	*	up	32793	fmep-default-BBAK9603
SNG-80:NULL	fma-default	*	up	32792	fmep-default-BBAK8728
Node-80:xe-0/0/22.0	fma1	V10	up	1	

Meaning Interfaces Node-84:xe-0/0/22.0 and Node-80:xe-0/0/22.0 are associated with the FMA, FMEP, and VLAN as configured.

Interfaces that are not configured for fabric OAM monitoring (NW-NG-0:NULL, RSNG-8384:NULL, SNG-60:NULL, and SNG-80:NULL) display an asterisk (*) in the VLAN column, and the default FMA and FMEP names in the Fabric-Maintenance Association and MEP Name columns.

Verifying Configuration of the Fabric OAM Flow Specification

Purpose Verify the configuration of the flow specifications.

Action Display the fabric OAM flow specification configuration.

```
root@qfabric> show oam fabric flow-specification
Flow specification name : flowspec1 Type : Ethernet Unicast IPv4
  Ethernet frame size : Unspecified
  Source-IP : 10.244.10.100
  Source-IP Mask : Unspecified
  Destination-IP : 10.244.10.110
  Destination-IP Mask : Unspecified
  Destination-mac : 0:0:80:8d:2d:15
  IP-protocol : Unspecified
  Source-L4-port : 60
  Destination-L4-port : 80
Flow specification name : flowspec2 Type : Ethernet Unicast IPv4
  Ethernet frame size : Unspecified
  Source-IP : 10.244.10.100
  Source-IP Mask : Unspecified
  Destination-IP : 10.244.10.111
  Destination-IP Mask : Unspecified
  Destination-mac : 0:0:80:8d:2d:17
  IP-protocol : Unspecified
  Source-L4-port : 60
  Destination-L4-port : 80
```

Meaning The output shows that flow specifications were configured as the user intended.

Verifying Operation of the Unicast ping Command

Purpose Verify that the fabric OAM unicast **ping** command works.

Action Issue the **ping fabric unicast-flow** command.

```
root@qfabric> ping fabric unicast-flow source-fmep-id 1 dest-fmep-id 2 flow-spec-name
flowspec1 fma-name fma1 count 3
Fabric flow ping between source Node-80 destination Node-84
received response from fmep-id 2...
received response from fmep-id 2...
received response from fmep-id 2...
sent 3 requests, received 3 responses

root@qfabric> ping fabric unicast-flow source-fmep-id 1 dest-fmep-id 2 fma-name
fma1 flow-spec-name flowspec2
Fabric flow ping between source Node-80 destination Node-84
received response from fmep-id 2...
sent 1 requests, received 1 responses
```

Meaning The fabric OAM unicast ping request from the source Node device (Node-80) to the destination Node device (Node-84) has been successful.

Related Documentation

- [Overview of Internal Fabric Monitoring on page 29](#)
- [fabric-maintenance-associations on page 239](#)

- [fabric-maintenance-end-points on page 240](#)
- [flow-specs on page 241](#)
- [show oam fabric flow-specification on page 411](#)
- [show oam fabric interfaces on page 414](#)

sFlow Technology

- [Configuring sFlow Technology on page 115](#)
- [Example: Monitoring Network Traffic Using sFlow Technology on page 116](#)

Configuring sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS fully supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

On the QFabric system, the sFlow monitoring global configuration that is defined on the Director device is distributed to Node groups that have sFlow sampling configured on the interfaces.

To configure sFlow features using the CLI:

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

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

The default UDP port assigned is 6343.

2. Enable sFlow technology on a specific interface:

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



NOTE: You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.

You cannot enable sFlow technology on a LAG interface (for example ae0), but you can enable sFlow technology on the member interfaces of the LAG (for example, xe-0/0/1).

3. Specify how often (in seconds) the sFlow agent polls all interfaces at the global level:

```
[edit protocols sflow]
user@host# set polling-interval seconds
```



NOTE: Specify 0 if you do not want to poll the interface.

4. Specify the rate at which packets are sampled at the global level. For example, configuring a **number** of 1000 sets a sample rate of 1 in 1000 packets.

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

5. (Optional) You can also configure the polling interval and sample rate at the interface level:

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



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

**Related
Documentation**

- [Example: Monitoring Network Traffic Using sFlow Technology on page 116](#)
- [Overview of sFlow Technology on page 35](#)

Example: Monitoring Network Traffic Using sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS fully supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

This example describes how to configure and use sFlow monitoring on a QFX3500 switch in standalone mode.

- [Requirements on page 117](#)
- [Overview on page 117](#)
- [Configuration on page 118](#)
- [Verification on page 119](#)

Requirements

This example uses the following hardware and software components:

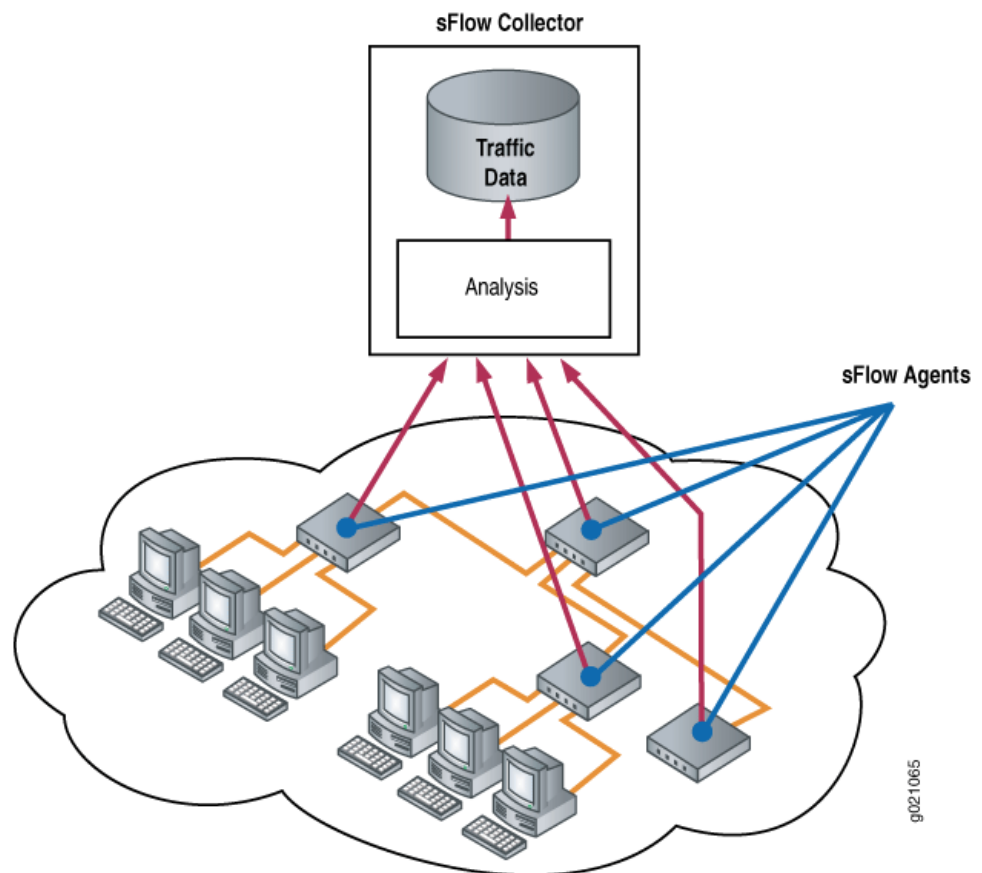
- Junos OS Release 11.3 or later
- One QFX3500 switch

Overview

An sFlow monitoring system consists of an sFlow agent embedded in the device and a centralized collector on the network. The two main activities of the sFlow agent are random sampling and statistics gathering. The sFlow agent combines interface counters and flow samples and sends them to the IP address and UDP destination port of the sFlow collector in UDP datagrams.

Figure 8 on page 117 depicts the basic elements of an sFlow system.

Figure 8: sFlow Technology Monitoring System



Configuration

CLI Quick Configuration To quickly configure sFlow technology, copy the following commands and paste them into the terminal window of the switch:

```
[edit protocols sflow]
set collector 10.204.32.46 udp-port 5600
set interfaces xe-0/0/1.0
set polling-interval 20
set sample-rate 1000
```

Step-by-Step Procedure To configure sFlow features using the CLI:

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

```
[edit protocols sflow]
user@switch# set collector 10.204.32.46 udp-port 5600
```

The default UDP port assigned is 6343.

2. Enable sFlow technology on a specific interface:

```
[edit protocols sflow]
user@switch# set interfaces xe-0/0/1.0
```



NOTE: You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.

You cannot enable sFlow technology on a LAG interface (for example, ae0), but you can enable sFlow technology on the member interfaces of the LAG (for example, xe-0/0/1).

3. Specify how often (in seconds) the sFlow agent polls all interfaces at the global level:

```
[edit protocols sflow]
user@switch# set polling-interval 20
```



NOTE: Specify 0 if you do not want to poll the interface.

4. Specify the rate at which packets must be sampled at the global level. The following example sets a sample rate of 1 in 1000 packets:

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

Results Check the results of the configuration:

```
[edit]
user@switch# show protocols
sflow {
  collector 10.204.32.46 {
    udp-port 5600;
```



```

}
interfaces xe-0/0/1.0 {
  polling-interval 20;
  sample-rate 1000;
}
}

```

Verification

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

- [Verifying That sFlow Technology Has Been Configured Properly on page 119](#)
- [Verifying That sFlow Technology Is Enabled on an Interface on page 119](#)
- [Verifying the sFlow Collector Configuration on page 120](#)

Verifying That sFlow Technology Has Been Configured Properly

Purpose Verify that sFlow technology has been configured properly.

Action Enter the **show sflow** operational mode command:

```

user@switch> show sflow
sFlow           : Enabled
Sample limit    : 300 packets/second
Polling interval : 20 second
Sample rate     : 1:1000
Agent ID        : 10.1.1.2

```



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

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

Verifying That sFlow Technology Is Enabled on an Interface

Purpose Verify that sFlow technology is enabled on interfaces and display the sampling parameters.

Action Enter the **show sflow interface** operational mode command:

```

user@switch> show sflow interface
Interface      Status      Sample    Polling
                rate      interval
xe-0/0/1.0     Enabled     1000      20

```

Meaning The output indicates that sFlow technology is enabled on the **Node1:xe-0/0/1.0** interface on the Node device with a sampling rate of 1000 and a polling interval of 20 seconds.

Verifying the sFlow Collector Configuration

Purpose Verify the sFlow collector configuration.

Action Enter the **show sflow collector** operational mode command:

```
user@switch> show sflow collector
Collector      Udp-port      No. of samples
address
10.204.32.46   5600          7516
```

Meaning The output displays the IP address of the collector, the UDP port, and the number of samples collected.

Related Documentation

- [Configuring sFlow Technology on page 115](#)
- [Overview of sFlow Technology on page 35](#)

CHAPTER 12

SNMP

- [Configuring SNMP on page 121](#)
- [Configuring the SNMP Community String on page 125](#)
- [Configuring SNMP Trap Groups on page 126](#)
- [Adding a Group of Clients to an SNMP Community on page 127](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 128](#)
- [Configuring MIB Views on page 129](#)
- [Configuring RMON Alarms and Events on page 130](#)
- [Configuring Health Monitoring on page 132](#)
- [Creating SNMPv3 Users on page 133](#)
- [Configuring Access Privileges for a Group on page 134](#)
- [Assigning a Security Name to a Group on page 136](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 137](#)
- [Configuring SNMP Informs on page 138](#)
- [Example: Configuring SNMP on page 139](#)

Configuring SNMP

SNMP is implemented in the Junos OS Software running on the QFX Series and OCX Series products. By default, SNMP is not enabled. To enable SNMP, you must include the SNMP configuration statements at the **[edit]** hierarchy level.

To configure the minimum requirements for SNMP, include the following statements at the **[edit]** hierarchy level of the configuration:

```
[edit]
snmp {
  community public;
}
```

To configure complete SNMP features, include the following statements at the **[edit]** hierarchy level of the configuration:

```
snmp {
  client-list client-list-name {
    ip-addresses;
```



```
}
community community-name {
  authorization authorization;
  client-list-name client-list-name;
  clients {
    address restrict;
  }
  logical-system logical-system-name {
    routing-instance routing-instance-name {
      clients {
        addresses;
      }
    }
  }
  routing-instance routing-instance-name {
    clients {
      addresses;
    }
  }
  view view-name;
}
contact contact;
description description;
filter-duplicates;
filter-interfaces;
health-monitor {
  falling-threshold integer;
  interval seconds;
  rising-threshold integer;
}
interface [ interface-names ];
location location;
name name;
nonvolatile {
  commit-delay seconds;
}
rmon {
  alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    request-type;
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
    syslog-subtag syslog-subtag;
    variable oid-variable;
  }
  event index {
    community community-name;
    description description;
    type type;
  }
}
```



```

history history-index {
    bucket-size number;
    interface interface-name;
    interval seconds;
    owner owner-name;
}
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regular-expression>;
    flag flag;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance routing-instance-name;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-level (authentication | none | privacy);

```



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



```

        notify-view view-name;
        read-view view-name;
        write-view view-name;
    }
}
}
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
}
view view-name {
    oid object-identifier (include | exclude);
}
}

```

**Related
Documentation**

- [Understanding the Implementation of SNMP on page 39](#)
- [snmp on page 330](#)

Configuring the SNMP Community String

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string in a Junos OS configuration, include the **community** statement at the **[edit snmp]** hierarchy level:

```

[edit snmp]
community name {
    authorization authorization;
    clients {
        default restrict;
        address restrict;
    }
    view view-name;
}

```

If the community name contains spaces, enclose it in quotation marks (" ").

The default authorization level for a community is **read-only**. To allow **Set** requests within a community, you need to define that community as **authorization read-write**. For **Set** requests, you also need to include the specific MIB objects that are accessible with read-write privileges using the **view** statement. The default view includes all supported MIB objects that are accessible with read-only privileges; no MIB objects are accessible with read-write privileges. For more information about the **view** statement, see [“Configuring MIB Views” on page 129](#).

The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. If no **clients** statement is present, all clients are allowed. For **address**, you must specify an IPv4 address, not a hostname. Include the **default restrict** option to deny access to all SNMP clients for which access is not explicitly granted. We recommend that you always include the **default restrict** option to limit SNMP client access to the local switch.



NOTE: Community names must be unique within each SNMP system.

**Related
Documentation**

- [Configuring SNMP on page 121](#)

Configuring SNMP Trap Groups

Before any SNMP traps can be sent, you must configure a trap group, the categories of traps the group can receive, and the targets (systems) that will receive the traps. To create and name an SNMP trap group, include the **trap-group** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, include the **destination-port** statement. The default destination port is port 162.

For each trap group that you define, you must include the **target** statement to define at least one system as the recipient of the SNMP traps in the trap group. Specify the IPv4 address of each recipient and not its hostname.

Specify the types of traps the trap group can receive in the **categories** statement.

A trap group can receive the following categories of traps:

- **authentication**—Authentication failures
- **chassis**—Chassis or environment notifications
- **configuration**—Configuration notifications
- **link**—Link-related notifications such as up-down transitions

- **remote-operations**—Remote operation notifications
- **startup**—System warm and cold starts

The **version** statement allows you to specify the SNMP version of the traps sent to targets of the trap group. If you specify **v1** only, SNMPv1 traps are sent. If you specify **v2** only, SNMPv2 traps are sent. If you specify **all**, both an SNMPv1 and an SNMPv2 trap are sent for every trap condition. For more information about the **version** statement, see [version](#).

Related Documentation

- *Standard SNMP Version 1 Traps*
- *Standard SNMP Version 2 Traps*
- *Juniper Networks Enterprise-Specific SNMP Version 1 Traps*
- *Juniper Networks Enterprise-Specific SNMP Version 2 Traps*

Adding a Group of Clients to an SNMP Community

Junos OS enables you to add one or more groups of clients to an SNMP community. You can include the **client-list-name** *name* statement at the **[edit snmp community community-name]** hierarchy level to add all the members of the client list or prefix list to an SNMP community.

To define a list of clients, include the **client-list** statement followed by the IP addresses of the clients at the **[edit snmp]** hierarchy level:

```
[edit snmp]
  client-list client-list-name {
    ip-addresses;
  }
```

You can configure a prefix list at the **[edit policy options]** hierarchy level. Support for prefix lists in the SNMP community configuration enables you to use a single list to configure the SNMP and routing policies. For more information about the **prefix-list** statement, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

To add a client list or prefix list to an SNMP community, include the **client-list-name** statement at the **[edit snmp community community-name]** hierarchy level:

```
[edit snmp community community-name]
  client-list-name client-list-name;
```



NOTE: The client list and prefix list must not have the same name.

The following example shows how to define a client list:

```
[edit]
snmp {
  client-list clentlist1 {
    10.1.1.1/32;
    10.2.2.2/32;
```



```
}  
}
```

The following example shows how to add a client list to an SNMP community:

```
[edit]  
snmp {  
  community community1 {  
    authorization read-only;  
    client-list-name clientlist1;  
  }  
}
```

The following example shows how to add a prefix list to an SNMP community:

```
[edit]  
policy-options {  
  prefix-list prefixlist {  
    10.3.3.3/32;  
    10.5.5.5/32;  
  }  
}  
snmp {  
  community community2 {  
    client-list-name prefixlist;  
  }  
}
```

- Related Documentation**
- [client-list on page 271](#)
 - [client-list-name on page 272](#)

Configuring the Interfaces on Which SNMP Requests Can Be Accepted

By default, all router or switch interfaces have SNMP access privileges. To limit the access through certain interfaces only, include the **interface** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]  
interface [ interface-names ];
```

Specify the names of any logical or physical interfaces that should have SNMP access privileges. Any SNMP requests entering the router or switch from interfaces not listed are discarded.

- Related Documentation**
- *Configuring SNMP on a Device Running Junos OS*
 - *Configuration Statements at the [edit snmp] Hierarchy Level*
 - *Example: Configuring Secured Access List Checking*
 - [Configuring SNMP on page 121](#)

Configuring MIB Views

SNMPv3 defines the concept of MIB views in RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. MIB views provide an agent better control over who can access specific branches and objects within its MIB tree. A view consists of a name and a collection of SNMP object identifiers, which are either explicitly included or excluded. Once defined, a view is then assigned to an SNMPv3 group or SNMPv1/v2c community (or multiple communities), automatically masking which parts of the agent's MIB tree members of the group or community can (or cannot) access.

By default, an SNMP community grants read access and denies write access to all supported MIB objects (even communities configured as **authorization read-write**). To restrict or grant read or write access to a set of MIB objects, you must configure a MIB view and associate the view with a community.

To create a MIB view and assign it to a community:

1. Configure a MIB view.

Although most network management systems use SNMPv3, Junos OS allows the use of MIB views with both SNMPv1 and SNMPv2c communities.

The **view** statement defines a MIB view and identifies a group of MIB objects. Each MIB object of a view has a common object identifier (OID) prefix. Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). A configuration statement uses a view to specify a group of MIB objects on which to define access. You can also use a wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, you must associate the view with a community.

To remove an OID completely, use the **delete view all oid oid-number** command but omit the **include** parameter.

```
[edit groups global snmp]
user@host# set view view-name oid object-identifier (include | exclude)
```

The following example creates a MIB view called ping-mib-view. The **oid** statement does not require a dot at the beginning of the object identifier. The **snmp view** statement includes the branch under the object identifier .1.3.6.1.2.1.80. This includes the entire DISMAN-PINGMIB subtree (as defined in RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*), which effectively permits access to any object under that branch.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid 1.3.6.1.2.1.80 include
```

The following example adds a second branch in the same MIB view.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid jnxPingMIB include
```

2. Assign a MIB view to a community that you want to control.


```
[edit groups global snmp community community-name]  
user@host# set view view-name
```

This example creates a new community ping-mib which has read-write access to create entries within the DISMAN-PING-MIB.

```
[edit groups global snmp community ping-mib]  
user@host# set authorization read-write
```

This example associate the MIB view created earlier with the new community.

```
[edit groups global snmp community ping-mib]  
user@host# set view ping-mib-view
```

3. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

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

4. Commit the configuration.

```
user@host# commit
```

5. To verify, make sure that any member of the ping-mib community has read/write access to the branches that you specified under ping-mib-view.

Related Documentation

- *PING MIB*
- *Configuring SNMP on a Device Running Junos OS*
- *Configuration Statements at the [edit snmp] Hierarchy Level*
- *Example: Ping Proxy MIB*
- *SNMP MIBs and Traps Reference*

Configuring RMON Alarms and Events

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

To configure RMON alarms and events using the CLI, perform these tasks:

1. [Configuring SNMP on page 131](#)
2. [Configuring an Event on page 131](#)
3. [Configuring an Alarm on page 132](#)

Configuring SNMP

To configure SNMP:

1. Grant read-only access to all SNMP clients:

```
[edit snmp]
user@switch# set community community-name authorization authorization
```

For example:

```
[edit snmp]
user@switch# set community public authorization read-only
```

2. Grant read-write access to the RMON and jnx-rmon MIBs:

```
[edit snmp]
user@switch# set view view-name oid object-identifier include
user@switch# set view view-name oid object-identifier include
user@switch# set community community-name authorization authorization view view-name
```

For example:

```
[edit snmp]
user@switch# set view rmon-mib-view oid .1.3.6.1.2.1.16 include
user@switch# set view rmon-mib-view oid .1.3.6.1.4.1.2636.13 include
user@switch# set community private authorization read-write view rmon-mib-view
```

OIDs 1.3.6.1.2.1.16 and 1.3.6.1.4.1.2636.13 correspond to the RMON and jnxRmon MIBs.

3. Configure an SNMP trap group:

```
[edit snmp]
user@switch# set trap-group group-name categories category
user@switch# set trap-group group-name targets address
```

For example:

```
[edit snmp]
user@switch# set trap-group rmon-trap-group categories rmon-alarm
user@switch# set trap-group rmon-trap-group targets 192.168.5.5
```

The trap group **rmon-trap-group** is configured to send RMON traps to 192.168.5.5.

Configuring an Event

To configure an event:

1. Configure an event index, community name, and type:

```
[edit snmp rmon]
user@switch# set event index community community-name typetype
```

For example:

```
[edit snmp rmon]
user@switch# set event 1 community rmon-trap-group type log-and-trap
```

The event community corresponds to the SNMP trap group and is not the same as an SNMP community. This event generates an SNMP trap and adds an entry to the **logTable** in the RMON MIB.

2. Configure a description for the event:

```
[edit snmp rmon]
user@switch# set event index description description
```


For example:

```
[edit snmp rmon]
user@switch# set event 1 description "rmon event"
```

Configuring an Alarm

To configure an alarm:

1. Configure an alarm index, the variable to monitor, the rising and falling thresholds, and the corresponding rising and falling events:

```
[edit snmp rmon]
user@switch# set alarm index variable oid-variable falling-threshold integer rising-threshold
integer rising-event-index index falling-event-index index
```

For example:

```
[edit snmp rmon]
user@switch# set alarm 5 variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 falling-threshold 75
rising-threshold 90 rising-event-index 1 falling-event-index 1
```

The variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 corresponds to the `jnxRmon` MIB object `jnxOperatingCPU`, which represents the CPU utilization of the Routing Engine. The falling and rising threshold integers are 75 and 90. The rising and falling events both generate the same event (event index 1).

2. Configure the sample interval and type and the alarm type:

```
[edit snmp rmon]
user@switch# set alarm index interval seconds sample-type (absolute-value | delta-value)
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm)
```

For example:

```
[edit snmp rmon]
user@switch# set alarm 5 interval 30 sample-type absolute-value
startup-alarm rising-or-falling-alarm
```

The absolute value of the monitored variable is sampled every 30 seconds. The initial alarm can occur because of rising above the rising threshold or falling below the falling threshold.

Related Documentation

- [Configuring SNMP on page 121](#)
- [Juniper Networks Enterprise-Specific MIBs](#)
- [Monitoring RMON MIB Tables on page 179](#)
- [RMON MIB Event, Alarm, Log, and History Control Tables on page 53](#)
- [Understanding RMON on page 51](#)

Configuring Health Monitoring

This topic describes how to configure the health monitor feature for QFX Series and OCX Series devices.

The health monitor feature extends the SNMP RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (such as file system usage,

CPU usage, and memory usage) and dynamic object instances (such as Junos OS processes).

To configure health monitoring:

1. Configure the health monitor:

```
[edit snmp]
user@switch# set health-monitor
```

2. Configure the falling threshold:

```
[edit snmp]
user@switch# set health-monitor falling-threshold percentage
```

For example:

```
user@switch# set health-monitor falling-threshold 85
```

3. Configure the rising threshold:

```
[edit snmp]
user@switch# set health-monitor rising-threshold percentage
```

For example:

```
user@switch# set health-monitor rising-threshold 75
```

4. Configure the interval:

```
[edit snmp]
user@switch# set health-monitor interval seconds
```

For example:

```
user@switch# set health-monitor interval 600
```

Related Documentation

- [Understanding Health Monitoring on page 55](#)
- [falling-threshold on page 283](#)
- [interval \(Health Monitor\) on page 293](#)
- [rising-threshold \(Health Monitor\) on page 316](#)

Creating SNMPv3 Users

For each SNMPv3 user, you can specify the username, authentication type, authentication password, privacy type, and privacy password. After a user enters a password, a key based on the engine ID and password is generated and is written to the configuration file. After the generation of the key, the password is deleted from this configuration file.



NOTE: You can configure only one encryption type for each SNMPv3 user.

To create users, include the **user** statement at the **[edit snmp v3 usm local-engine]** hierarchy level:

```
[edit snmp v3 usm local-engine]
user username;
```

username is the name that identifies the SNMPv3 user.

To configure user authentication and encryption, include the following statements at the **[edit snmp v3 usm local-engine user username]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-md5 {
  authentication-password authentication-password;
}
authentication-sha {
  authentication-password authentication-password;
}
authentication-none;
privacy-aes128 {
  privacy-password privacy-password;
}
privacy-des {
  privacy-password privacy-password;
}
privacy-3des {
  privacy-password privacy-password;
}
privacy-none;
```

Related Documentation

- [Complete SNMPv3 Configuration Statements](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50](#)
- [Example: Creating SNMPv3 Users](#)
- [Example: SNMPv3 Configuration](#)

Configuring Access Privileges for a Group

In SNMPv3, you can configure a group that sets the same access privileges for one or more users. Configuring a group includes defining the security model and security level, and associating one or more MIB view permissions for the group.



NOTE: You must associate at least one MIB view with the group. You can associate multiple MIB views (read, notify, write) to authorize different permissions based on the view. The view name cannot exceed 32 characters.

To configure access privileges for a group:

1. To configure the group:

```
[edit snmp v3 vacm access]
user@switch# edit group group-name
```


2. To configure the context prefix of the SNMP instance for the group:

```
[edit snmp v3 vacm access group group-name]
user@switch# edit (default-context-prefix | context-prefix context-prefix)
```

For example, to configure the default context prefix:

```
[edit snmp v3 vacm access group group-name]
user@switch# edit default-context-prefix
```

3. To configure the security model:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix)]
user@switch# edit security-model (any | usm | v1 | v2c)
```

For example, to configure the SNMPv3 user-based security model (USM):

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix)]
user@switch# edit security-model usm
```

4. To configure the security level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c)]
user@switch# edit security-level (authentication | none | privacy)
```

For example, to configure a security level requiring user authentication and encryption:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c)]
user@switch# edit security-level privacy
```



NOTE: Access privileges are granted to all packets with a security level equal to or greater than that configured. If you are configuring the SNMPv1 or v2c security model, use *none* as your security level. If you are configuring the SNMPv3 security model (USM), use the *authentication*, *none*, or *privacy* security level.

5. (Optional) To associate a read-only MIB view with an SNMP group:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication |
none | privacy)]
user@switch# edit read-view view-name
```

6. (Optional) To associate a MIB view with an SNMP notification permission for an SNMP group:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication |
none | privacy)]
user@switch# edit notify-view view-name
```

7. (Optional) To associate a MIB view with write permission for an SNMP group:


```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication |
none | privacy)]
user@switch# edit write-view view-name
```

- Related Documentation**
- [SNMPv3 Overview on page 49](#)
 - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50](#)

Assigning a Security Name to a Group

In SNMPv3, each username is associated with a security name. The security name, together with the SNMP engine ID, is included in SNMP messages to ensure messaging security.

Before you assign a security name to a group, first create the security name. For an SNMPv3 client, the security name is the username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 or v2c clients, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Assigning a security name to a group includes configuring a security model for the group, assigning the security name to the group, and configuring the group.

To assign an SNMP security name to a group:

1. To configure a security model for the group:

```
[edit snmp v3 vacm security-to-group]
user@switch# edit security-model (usm | v1 | v2c)
```

For example, to configure the SNMPv3 user-based security model (USM):

```
[edit snmp v3 vacm security-to-group]
user@switch# edit security-model usm
```

2. To associate the security name with a group:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
user@switch# edit security-name security-name
```

3. To configure a group of SNMPv3 security names with the same security policy:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name
security-name]
user@switch# edit group group-name
```

- Related Documentation**
- [Creating SNMPv3 Users on page 133](#)
 - [group \(Associating a Security Name\) on page 287](#)
 - [security-model \(Group\) on page 324](#)
 - [security-name \(Community String\) on page 326](#)
 - [security-name \(Security Group\) on page 327](#)

Configuring SNMPv3 Traps on a Device Running Junos OS

In SNMPv3, you create traps and informs by configuring the **notify**, **target-address**, and **target-parameters** parameters. Traps are unconfirmed notifications, whereas informs are confirmed notifications. This section describes how to configure SNMP traps. For information about configuring SNMP informs, see “[Configuring SNMP Informs](#)” on page 138.

The target address defines a management application’s address and parameters to be used in sending notifications. Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target. SNMPv3 also lets you define SNMPv1 and SNMPv2c traps.



NOTE: When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Access privileges are configured at the `[edit snmp v3 vacm access]` and `[edit snmp v3 vacm security-to-group]` hierarchy levels.

To configure SNMP traps, include the following statements at the `[edit snmp v3]` hierarchy level:

```
[edit snmp v3]
  notify name {
    tag tag-name;
    type trap;
  }
  notify-filter name {
    oid object-identifier (include | exclude);
  }
  target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system (SNMP) logical-system;
    port port-number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | v3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
}
```

- Related Documentation**
- [Configuring the SNMPv3 Trap Notification](#)
 - [Configuring the Trap Notification Filter](#)
 - [Configuring the Trap Target Address](#)

- *Defining and Configuring the Trap Target Parameters*
- [Configuring SNMP Informs on page 138](#)
- *Configuring the Remote Engine and Remote User*
- *Configuring the Inform Notification Type and Target Address*
- *Complete SNMPv3 Configuration Statements*
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50](#)

Configuring SNMP Informs

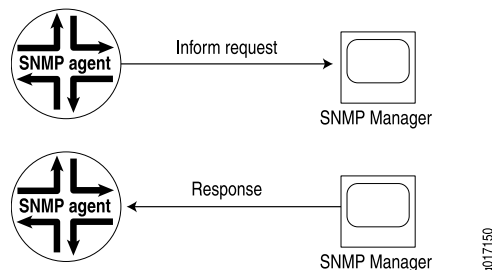
Junos OS supports two types of notifications: traps and informs. With traps, the receiver does not send any acknowledgment when it receives a trap. Therefore, the sender cannot determine if the trap was received. A trap may be lost because a problem occurred during transmission. To increase reliability, an inform is similar to a trap except that the inform is stored and retransmitted at regular intervals until one of these conditions occurs:

- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted and the agent discards the inform message.

If the sender never receives a response, the inform can be sent again. Thus, informs are more likely to reach their intended destination than traps are. Informs use the same communications channel as traps (same socket and port) but have different protocol data unit (PDU) types.

Informs are more reliable than traps, but they consume more network, router, and switch resources (see [Figure 9 on page 138](#)). Unlike a trap, an inform is held in memory until a response is received or the timeout is reached. Also, traps are sent only once, whereas an inform may be retried several times. Use informs when it is important that the SNMP manager receive all notifications. However, if you are more concerned about network traffic, or router and switch memory, use traps.

Figure 9: Inform Request and Response



For information about configuring SNMP traps, see [“Configuring SNMPv3 Traps on a Device Running Junos OS” on page 137](#).

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 137](#)
- *Configuring the Remote Engine and Remote User*

- *Configuring the Inform Notification Type and Target Address*
- *Complete SNMPv3 Configuration Statements*
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50](#)

Example: Configuring SNMP

By default, SNMP is disabled on devices running Junos OS. This example describes the steps for configuring SNMP on the QFabric system.

- [Requirements on page 139](#)
- [Overview on page 139](#)
- [Configuration on page 139](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- Network management system (NMS) (running the SNMP manager)
- QFabric system (running the SNMP agent) with multiple Node devices

Overview

Because SNMP is disabled by default on devices running Junos OS, you must enable SNMP on your device by including configuration statements at the **[edit snmp]** hierarchy level. At a minimum, you must configure the **community public** statement. The community defined as public grants read-only access to MIB data to any client.

If no **clients** statement is configured, all clients are allowed. We recommend that you always include the **restrict** option to limit SNMP client access to the switch.

The network topology in this example includes an NMS, a QFabric system with four Node devices, and external SNMP servers that are configured for receiving traps.

Configuration

CLI Quick Configuration

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

```
set snmp name "snmp qfabric" description "qfabric0 switch"
set snmp location "Lab 4 Row 11" contact "qfabric-admin@qfabric0"
set snmp community public authorization read-only
set snmp client-list list0 192.168.0.0/24
set snmp community public client-list-name list0
set snmp community public clients 192.170.0.0/24 restrict
set snmp trap-group "qf-traps" destination-port 155 targets 192.168.0.100
```


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

To configure SNMP on the QFabric system:



NOTE: If the name, description, location, contact, or community name contains spaces, enclose the text in quotation marks (" ").

1. Configure the SNMP system name:

```
[edit snmp]
user@switch# set name "snmp qfabric"
```

2. Specify a description.

```
[edit snmp]
user@switch# set description "qfabric0 system"
```

This string is placed into the MIB II sysDescription object.

3. Specify the physical location of the QFabric system.

```
[edit snmp]
user@switch# set location "Lab 4 Row 11"
```

This string is placed into the MIB II sysLocation object.

4. Specify an administrative contact for the SNMP system.

```
[edit snmp]
user@switch# set contact "qfabric-admin@qfabric0"
```

This name is placed into the MIB II sysContact object.

5. Specify a unique SNMP community name and the read-only authorization level.



NOTE: The read-write option is not supported on the QFabric system.

```
[edit snmp]
user@switch# set community public authorization read-only
```

6. Create a client list with a set of IP addresses that can use the SNMP community.

```
[edit snmp]
user@switch# set client-list list0 192.168.0.0/24
user@switch# set community public client-list-name list0
```

7. Specify IP addresses of clients that are restricted from using the community.

```
[edit snmp]
user@switch# set community public clients 192.170.0.0/24 restrict
```

8. Configure a trap group, destination port, and a target to receive the SNMP traps in the trap group.


```
[edit snmp]
user@switch# set trap-group "qf-traps" destination-port 155 targets 192.168.0.100
```



NOTE: You do not need to include the `destination-port` statement if you use the default port 162.

The trap group `qf-traps` is configured to send traps to 192.168.0.100.

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

```
[edit]
user@switch# show
snmp {
  name "snmp qfabric";
  description "qfabric0 system";
  location "Lab 4 Row 11";
  contact "qfabric-admin@qfabric0";
  client-list list0 {
    192.168.0.0/24;
  }
  community public {
    authorization read-only;
    clients {
      197.170.0.0/24 restrict;
    }
  }
  trap-group qf-traps {
    destination-port 155;
    targets {
      192.168.0.100;
    }
  }
}
```

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

- Related Documentation**
- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)
 - [snmp on page 330](#)

CHAPTER 13

System Log Messages

- [Junos OS Minimum System Logging Configuration on page 144](#)
- [Junos OS System Log Configuration Statements on page 144](#)
- [Adding a Text String to System Log Messages Directed to a Remote Destination on page 145](#)
- [Directing System Log Messages to a Log File on page 146](#)
- [Directing System Log Messages to a Remote Machine on page 147](#)
- [Directing System Log Messages to a User Terminal on page 147](#)
- [Directing System Log Messages to the Console on page 148](#)
- [Disabling the System Logging of a Facility on page 148](#)
- [Displaying a Log File from a Single-Chassis System on page 149](#)
- [Including Priority Information in System Log Messages on page 150](#)
- [Including the Year or Millisecond in Timestamps on page 151](#)
- [Logging Messages in Structured-Data Format on page 152](#)
- [Interpreting Messages Generated in Structured-Data Format on page 153](#)
- [Interpreting Messages Generated in Standard Format on page 156](#)
- [Specifying Log File Size, Number, and Archiving Properties on page 157](#)
- [Specifying the Facility and Severity of Messages to Include in the Log on page 158](#)
- [Junos OS System Logging Facilities and Message Severity Levels on page 159](#)
- [Default Facilities for System Log Messages Directed to a Remote Destination on page 160](#)
- [Alternate Facilities for System Log Messages Directed to a Remote Destination on page 161](#)
- [Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination on page 162](#)
- [Using Regular Expressions to Refine the Set of Logged Messages on page 164](#)
- [Examples: Configuring System Logging on page 166](#)
- [Examples: Assigning an Alternative Facility on page 168](#)
- [Example: Configuring System Log Messages on page 169](#)

Junos OS Minimum System Logging Configuration

To record or view system log messages, you must include the **syslog** statement at the **[edit system]** hierarchy level. Specify at least one destination for the messages, as described in [Table 23 on page 144](#). For more information about the configuration statements, see *Single-Chassis System Logging Configuration Overview*.

Table 23: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements
File	<pre>[edit system syslog] file filename { facility severity; }</pre>
Terminal session of one, several, or all users	<pre>[edit system syslog] user (username *) { facility severity; }</pre>
Router or switch console	<pre>[edit system syslog] console { facility severity; }</pre>
Remote machine or the other Routing Engine on the router or switch	<pre>[edit system syslog] host (hostname other-routing-engine) { facility severity; }</pre>

Related Documentation

- [Junos OS System Log Overview](#)
- [Overview of Junos OS System Log Messages on page 89](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Junos OS System Log Configuration Statements

To configure the switch to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites (ftp-url <password password>) > <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
```



```

    match "regular-expression";
    structured-data {
        brief;
    }
}
host hostname {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string
    match "regular-expression";
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {
    facility severity;
    match "regular-expression";
}
}

```

**Related
Documentation**

- [Overview of Junos OS System Log Messages on page 89](#)

Adding a Text String to System Log Messages Directed to a Remote Destination

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the **log-prefix** statement at the **[edit system syslog host]** hierarchy level:

```

[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;

```

The string can contain any alphanumeric or special character except the equal sign (=) and the colon (:). It also cannot include the space character; do not enclose the string in quotation marks (" ") in an attempt to include spaces in it.

The Junos OS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

The following example shows how to add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine hardware-logger.mycompany.com:

```

[edit system syslog]
host hardware-logger.mycompany.com {
    any info;
    log-prefix M120;
}

```

When these configuration statements are included on an M120 router called origin1, a message in the system log on hardware-logger.mycompany.com looks like the following:

Mar 9 17:33:23 origin1 M120:mgd[477]: UI_CMDLINE_READ_LINE: user 'root', command 'run show version'

Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Specifying Log File Size, Number, and Archiving Properties on page 157](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Directing System Log Messages to a Log File

To direct system log messages to a file in the `/var/log` directory of the local Routing Engine, include the `file` statement at the `[edit system syslog]` hierarchy level:

```
[edit system syslog]
file filename {
  facility severity;
  archive <archive-sites (ftp-url <password password>)> <files number> <size size>
    <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
no-world-readable>;
  explicit-priority;
  match "regular-expression";
  structured-data {
    brief;
  }
}
```

For the list of facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*.

To prevent log files from growing too large, the Junos OS system logging utility by default writes messages to a sequence of files of a defined size. By including the `archive` statement, you can configure the number of files, their maximum size, and who can read them, either for all log files or for a certain log file. For more information, see [“Specifying Log File Size, Number, and Archiving Properties” on page 157](#).

For information about the following statements, see the indicated sections:

- `explicit-priority`—See [“Including Priority Information in System Log Messages” on page 150](#)
- `match`—See [“Using Regular Expressions to Refine the Set of Logged Messages” on page 164](#)
- `structured-data`—See *Logging Messages in Structured-Data Format*

Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Overview of Junos OS System Log Messages on page 89](#)
- [Logging Messages in Structured-Data Format on page 152](#)
- [Examples: Configuring System Logging](#)
- [Examples: Configuring System Logging on page 166](#)

Directing System Log Messages to a Remote Machine

To direct system log messages to a remote machine, include the **host** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
}
source-address source-address;
```

To direct system log messages to a remote machine, include the **host hostname** statement to specify the remote machine's IP version 4 (IPv4) address or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks switch. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

For the list of logging facilities and severity levels to configure under the **host** statement, see *Specifying the Facility and Severity of Messages to Include in the Log*.

To record facility and severity level information in each message, include the **explicit-priority** statement. For more information, see [“Including Priority Information in System Log Messages” on page 150](#).

For information about the **match** statement, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 164](#).

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the switch that is reported in the messages as their source. In each **host** statement, you can also include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message.

Related Documentation

- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Directing System Log Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the **user** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
user (username | *) {
  facility severity;
  match "regular-expression";
}
```


Specify one or more Junos OS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*. For information about the **match** statement, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 164.

- Related Documentation**
- *Single-Chassis System Logging Configuration Overview*
 - [Overview of Single-Chassis System Logging Configuration on page 89](#)
 - *Examples: Configuring System Logging*
 - [Examples: Configuring System Logging on page 166](#)

Directing System Log Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the **console** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
  console {
    facility severity;
  }
```

For the list of logging facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*.

- Related Documentation**
- *Single-Chassis System Logging Configuration Overview*
 - [Overview of Single-Chassis System Logging Configuration on page 89](#)
 - *Examples: Configuring System Logging*
 - [Examples: Configuring System Logging on page 166](#)

Disabling the System Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the **facility none** statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the **any severity** statement and then a **facility none** statement for each facility that you do not want to log. For example, the following logs all messages at the **error** level or higher to the console, except for messages from the **daemon** and **kernel** facilities. Messages from those facilities are logged to the file **>/var/log/internals** instead:

```
[edit system syslog]
  console {
    any error;
    daemon none;
    kernel none;
  }
```



```
file internals {
  daemon info;
  kernel info;
}
```

- Related Documentation**
- *Single-Chassis System Logging Configuration Overview*
 - [Overview of Single-Chassis System Logging Configuration on page 89](#)

Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue the following commands:

```
user@switch> show log log-filename
user@switch> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine.

The following example shows the output from the **show log messages** command:

```
user@switch1> show log messages
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 1
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 2
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 3
...
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Management
process): new instance detected (variable: sysApp1ElmtRunMemory.5.6.2293)
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Command-line
interface): new instance detected (variable: sysApp1ElmtRunMemory.5.8.2292)
...
Nov  4 12:08:30 switch1 rpdf[957]: task_connect: task BGP_100.10.10.1.6+179 addr
10.10.1.6+179: Can't assign requested
address
Nov  4 12:08:30 switch1 rpdf[957]: bgp_connect_start: connect 10.10.1.6 (Internal
AS 100): Can't assign requested address
Nov  4 12:10:24 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'exit '
Nov  4 12:10:27 switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
configuration mode
Nov  4 12:10:31 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'show log messages'
```

The following example shows the output from the **file show** command. The file in the pathname **/var/log/processes** has been previously configured to include messages from the daemon facility.

```
user@switch1> file show /var/log/processes
Feb 22 08:58:24 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 22 20:35:07 switch1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
trap_throttle_timer_handler: cleared all throttled traps
```



```
Feb 23 07:34:56 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 23 07:38:19 switch1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
SNMP trap: cold start
...
```

**Related
Documentation**

- [Interpreting Messages Generated in Standard Format on page 156](#)
- [Interpreting Messages Generated in Structured-Data Format on page 153](#)

Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```



NOTE: Messages logged in structured-data format include priority information by default. If you include the **structured-data** statement at the **[edit system syslog file *filename*]** hierarchy level along with the **explicit-priority** statement, the **explicit-priority** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see *Logging Messages in Structured-Data Format*. For information about the contents of a structured-data message, see the *Junos OS System Log Messages Reference*.

To include priority information in messages directed to a remote machine or the other Routing Engine, include the **explicit-priority** statement at the **[edit system syslog host (*hostname* | other-routing-engine)]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```



NOTE: The **other-routing-engine** option does not apply to the QFX Series or OCX Series.

The priority recorded in a message always indicates the original, local facility name. If the **facility-override** statement is included for messages directed to a remote destination, the Junos OS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see [“Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination” on page 162](#).

When the **explicit-priority** statement is included, the Junos OS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

FACILITY-severity[-TAG]

(The tag is a unique identifier assigned to some Junos OS system log messages; for more information, see the *Junos OS System Log Messages Reference*.)

In the following example, the **CHASSISD_PARSE_COMPLETE** message belongs to the **daemon** facility and is assigned severity **info** (6):

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE:
Using new configuration
```

When the **explicit-priority** statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new
configuration
```

For more information about message formatting, see the *Junos OS System Log Messages Reference*.

Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- [Overview of Single-Chassis System Logging Configuration on page 89](#)
- *Examples: Configuring System Logging*

Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 15:36:30
```

To include the year, the millisecond, or both, in the timestamp, include the **time-format** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

The modified timestamp is used in messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2010):

```
Aug 21 15:36:30.401 2010
```




NOTE: By default, messages logged in structured-data format include the year and millisecond. If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the time-format statement, the time-format statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see “[Logging Messages in Structured-Data Format](#)” on page 152. For information about interpreting messages in a structured-data format, see “[Interpreting Messages Generated in Structured-Data Format](#)” on page 153.

Logging Messages in Structured-Data Format

You can log messages to a file in structured-data format instead of the standard Junos OS format. The structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft **draft-ietf-syslog-protocol-21.txt**. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the **structured-data** statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]  
  facility severity;  
  structured-data {  
    brief;  
  }
```

The optional **brief** statement suppresses the English-language text that appears by default at the end of a message to describe the error or event. For information about the fields in a structured-data-format message, see “[Interpreting Messages Generated in Structured-Data Format](#)” on page 153.

The structured format is used for all messages logged to the file that are generated by a Junos OS process or software library.



NOTE: If you include either or both of the explicit-priority and time-format statements along with the structured-data statement, they are ignored. These statements apply to the standard Junos OS system log format, not to structured-data format.

Interpreting Messages Generated in Structured-Data Format

By default, Junos OS processes and software libraries write messages to the system log file in structured-data format. For information about the **structured-data** statement, see *Logging Messages in Structured-Data Format*.

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

```
<priority code>version timestamp hostname process processID TAG [junos@2636.platform
variable-value-pairs] message-text
```

Table 24 on page 153 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 24: Fields in Structured-Data Messages

Field	Description	Examples
<priority code>	Number that indicates the facility and severity of a message. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see <i>Specifying the Facility and Severity of Messages to Include in the Log</i> .	<165> for a message from the pfe facility (facility=20) with severity notice (severity=5).
version	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version
timestamp	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> YYYY-MM-DDTHH:MM:SS.MSZ is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC) YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC 	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719-08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
hostname	Name of the host that originally generated the message.	switch1

Table 24: Fields in Structured-Data Messages (*continued*)

Field	Description	Examples
<i>process</i>	Name of the Junos OS process that generated the message.	mgd
<i>processID</i>	UNIX process ID (PID) of the Junos process that generated the message.	3046
<i>TAG</i>	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
<i>junos@2636.platform</i>	An identifier for the type of hardware platform that generated the message. The junos@2636 prefix indicates that the platform runs the Junos OS. It is followed by a dot-separated numerical identifier for the platform type.	junos@2636.1.1.1.2.18
<i>variable-value-pairs</i>	A variable-value pair for each element in the <i>message-text</i> string that varies depending on the circumstances that triggered the message. Each pair appears in the format <i>variable</i> = " <i>value</i> ".	username="regress"
<i>message-text</i>	English-language description of the event or error (omitted if the brief statement is included at the [edit system syslog file <i>filename</i> structured-data] hierarchy level).	User 'regress' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="regress"] User 'regress' exiting configuration mode
```

When the brief statement is included at the [edit system syslog file *filename* structured-data] hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="regress"]
```

Table 25 on page 155 maps the codes that appear in the *priority-code* field to facility and severity level.



NOTE: Not all of the facilities and severities listed in Table 25 on page 155 can be included in statements at the [edit system syslog] hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see *Specifying the Facility and Severity of Messages to Include in the Log*.

Table 25: Facility and Severity Codes in the priority-code Field

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103
security (13)	104	105	106	107	108	109	110	111
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Interpreting Messages Generated in Standard Format

The syntax of a standard-format message generated by a Junos OS process or subroutine library depends on whether it includes priority information:

- When the **explicit-priority** statement is included at the `[edit system syslog file filename]` or `[edit system syslog host hostname]` hierarchy level, a system log message has the following syntax:

```
timestamp message-source: %facility-severity-TAG: message-text
```

- When directed to the console or to users, or when the **explicit-priority** statement is not included for files or remote hosts, a system log message has the following syntax:

```
timestamp message-source: TAG: message-text
```

Table 26 on page 156 describes the message fields.

Table 26: Fields in Standard-Format Messages

Field	Description
<i>timestamp</i>	Time at which the message was logged.
<i>message-source</i>	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields: hostname, process and process ID (PID). If the process does not report its PID, the PID is not displayed. The message source subfields are displayed in the following format: <i>hostname process[process-ID]</i>
<i>facility</i>	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: Facility Codes Reported in Priority Information in “Including Priority Information in System Log Messages” on page 150.
<i>severity</i>	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table: Numerical Codes for Severity Levels Reported in Priority Information in “Including Priority Information in System Log Messages” on page 150.
<i>TAG</i>	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix. Not all processes on a routing platform use tags, so this field does not always appear.
<i>message-text</i>	Text of the message.

Specifying Log File Size, Number, and Archiving Properties

To prevent log files from growing too large, by default the Junos system logging utility writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for EX Series switches and J Series routers
- 1 megabyte (MB) for M Series, MX Series, and T Series routers
- 10 MB for TX Matrix or TX Matrix Plus routers
- 1 MB for the QFX Series and OCX Series

When an active log file called **logfile** reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file **logfile.0.gz**. The logging utility then opens and writes to a new active file called **logfile**. This process is also known as file rotation. When the new **logfile** reaches the configured maximum size, **logfile.0.gz** is renamed **logfile.1.gz**, and the new **logfile** is closed, compressed, and renamed **logfile.0.gz**. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached and when the size of the active file reaches the configured maximum size, the contents of the last archived file are overwritten by the current active file. The logging utility by default also limits the users who can read log files to the **root** user and users who have the Junos OS **maintenance** permission.

Junos OS provides a configuration statement **log-rotate-frequency** that configures the system log file rotation frequency by configuring the time interval for checking the log file size. The frequency can be set to a value of 1 minute through 59 minutes. The default frequency is 15 minutes.

To configure the log rotation frequency, include the **log-rotate-frequency** statement at the **[edit system syslog]** hierarchy level.

You can include the **archive** statement to change the maximum size of each file, how many archive files are created, and who can read log files.

To configure values that apply to all log files, include the **archive** statement at the **[edit system syslog]** hierarchy level:

```
archive <files number> <size size> <world-readable | no-world-readable>;
```

To configure values that apply to a specific log file, include the **archive** statement at the **[edit system syslog file filename]** hierarchy level:

```
archive <archive-sites (ftp-url <password password>)> <files number> <size size>
  <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
  no-world-readable>;
```

archive-sites site-name specifies a list of archive sites that you want to use for storing files. The **site-name** value is any valid FTP URL to a destination. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list,

moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the specified log filename. For information about how to specify valid FTP URLs, see *Format for Specifying Filenames and URLs in Junos OS CLI Commands*.

binary-data Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems). To restore the default setting, include the **no-binary-data** statement.

files number specifies the number of files to create before the oldest file is overwritten. The value can be from 1 through 1000.

size size specifies the maximum size of each file. The value can be from 64 KB (64k) through 1 gigabyte (1g); to represent megabytes, use the letter **m** after the integer. There is no space between the digits and the **k**, **m**, or **g** units letter.

start-time "YYYY-MM-DD.hh:mm" defines the date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval interval defines the amount of time the current log file remains open (even if it has not reached the maximum possible size) and receives new statistics before it is closed and transferred to an archive site. This interval value can be from 5 through 2880 minutes.

world-readable enables all users to read log files. To restore the default permissions, include the **no-world-readable** statement.

**Related
Documentation**

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a *facility*, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level or higher are logged to the destination:

```
[edit system syslog]
(console | file filename | host destination | user username) {
    facility severity;
}
```

**Related
Documentation**

- [Junos OS System Logging Facilities and Message Severity Levels on page 159](#)

- *Single-Chassis System Logging Configuration Overview*
- *Examples: Configuring System Logging*
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Junos OS System Logging Facilities and Message Severity Levels

[Table 27 on page 159](#) lists the Junos system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 27: Junos OS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Changes to the Junos OS configuration
conflict-log	Specified configuration is invalid on the router type
daemon	Actions performed or errors encountered by system processes
dfc	Events related to dynamic flow capture
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
kernel	Actions performed or errors encountered by the Junos OS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by user-space processes

[Table 28 on page 160](#) lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see [“Disabling the System Logging of a Facility” on page 148](#).

Table 28: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
none	Disables logging of the associated facility to a destination
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard errors
error	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest

Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- [Overview of Single-Chassis System Logging Configuration on page 89](#)
- *Examples: Configuring System Logging*

Default Facilities for System Log Messages Directed to a Remote Destination

Table 29 on page 160 lists the default alternative facility name next to the Junos OS-specific facility name for which it is used. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 29: Default Facilities for Messages Directed to a Remote Destination

Junos OS-specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7

Table 29: Default Facilities for Messages Directed to a Remote Destination (*continued*)

Junos OS—specific Local Facility	Default Facility When Directed to Remote Destination
pfe	local4

Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Alternate Facilities for System Log Messages Directed to a Remote Destination

Table 30 on page 161 lists the facilities that you can specify in the **facility-override** statement.

Table 30: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the Junos OS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by user-space processes

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility

names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

Related Documentation

- *Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination*
- *Single-Chassis System Logging Configuration Overview*
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

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

Some facilities assigned to messages logged on the local router or switch have Junos OS-specific names (see [Table 27 on page 159](#)). In the recommended configuration, a remote machine designated at the **[edit system syslog host *hostname*]** hierarchy level is not a Juniper Networks router or switch, so its syslogd utility cannot interpret the Junos OS-specific names. To enable the standard syslogd utility to handle messages from these facilities when messages are directed to a remote machine, a standard **localX** facility name is used instead of the Junos OS-specific facility name.

[Table 29 on page 160](#) lists the default alternative facility name next to the Junos OS-specific facility name it is used for.

The syslogd utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks router or switch or the remote machine itself). For example, the following statements in the configuration of the router called **local-router** direct messages from the **authorization** facility to the remote machine *monitor.mycompany.com*:

```
[edit system syslog]
host monitor.mycompany.com {
  authorization info;
}
```

The default alternative facility for the local **authorization** facility is also **authorization**. If the syslogd utility on **monitor** is configured to write messages belonging to the **authorization** facility to the file **/var/log/auth-attempts**, then the file contains the messages generated when users log in to **local-router** and the messages generated when users log in to **monitor**. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the **auth-attempts** file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on **local-router** when they are directed to **monitor**. You can then configure the syslogd utility on **monitor** to write messages with the alternative facility to a different file from messages generated on **monitor** itself.

To change the facility used for all messages directed to a remote machine, include the **facility-override** statement at the **[edit system syslog host *hostname*]** hierarchy level:

```
[edit system syslog host hostname]
```



```
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the **localX** facilities. On the remote machine, you must also configure the syslogd utility to handle the messages in the desired manner.

[Table 30 on page 161](#) lists the facilities that you can specify in the **facility-override** statement.

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

The following example shows how to log all messages generated on the local router at the error level or higher to the local0 facility on the remote machine called monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
  any error;
  facility-override local0;
}
```

The following example shows how to configure routers located in California and routers located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned to alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routers to aggregate messages in the local0 facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local0;
}
```

- Configure New York routers to aggregate messages in the local2 facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local2;
}
```

On central-logger, you can then configure the system logging utility to write messages from the local0 facility to the file **change-log** and the messages from the local2 facility to the file **new-york-config**.

Related Documentation

- [Table 29 on page 160](#)
- [Alternate Facilities for System Log Messages Directed to a Remote Destination on page 161](#)

- *Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination*
- [Examples: Assigning an Alternative Facility on page 168](#)

Using Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

To specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the **match** statement and specify the regular expression which the text string must match:

```
match "regular-expression";
```

You can include this statement at the following hierarchy levels:

- **[edit system syslog file *filename*]** (for a file)
- **[edit system syslog user (*username* | *)]** (for a specific user session or for all user sessions on a terminal)
- **[edit system syslog host (*hostname* | other-routing-engine)]** (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, <http://www.ieee.org>).

[Table 31 on page 164](#) specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term *term* refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.



NOTE: The match statement is not case-sensitive.

Table 31: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
(pipe)	One of the terms that appears on either side of the pipe operator.

Table 31: Regular Expression Operators for the match Statement (*continued*)

Operator	Matches
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS-specific.
^ (caret)	Start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
\$ (dollar sign)	End of a line.
[] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.
() (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Using Regular Expressions

Filter messages that belong to the **interactive-commands** facility, directing those that include the string **configure** to the terminal of the root user:

```
[edit system syslog]
user root {
  interactive-commands any;
  match ".*configure.*";
}
```

Messages like the following appear on the **root** user's terminal when a user issues a **configure** command to enter configuration mode:

```
timestamp router-name mgd[PID]: UI_CMDLINE_READ_LINE: User 'user', command
'configure private'
```

Filter messages that belong to the **daemon** facility and have a severity of **error** or higher, directing them to the file **/var/log/process-errors**. Omit messages generated by the SNMP process (snmpd), instead directing them to the file **/var/log/snmpd-errors**:

```
[edit system syslog]
file process-errors {
  daemon error;
  match "!(.*snmpd.*)";
}
file snmpd-errors {
  daemon error;
  match ".*snmpd.*";
}
```

Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Overview of Single-Chassis System Logging Configuration on page 89](#)

- *Examples: Configuring System Logging*
- [Examples: Configuring System Logging on page 166](#)

Examples: Configuring System Logging

The system log provides an excellent way of tracking all management activity on the switch by recording events such as user authentication, access authorization, and command execution. Logged command executions include commands entered by users at the CLI prompt or by client applications such as the Junos XML protocol or NETCONF XML client. Because system log files contain information about commands executed on the switch and the user who executed the commands, checking system log files for failed authentication events can help identify attempts to hack in to the switch. You can also analyze network activity by correlating executed commands with events and changes that occurred on the network at a particular time.

System log files are stored locally on the switch in the default `/var/log` directory.

The following example shows how to configure system log messages to record all commands entered by users and all authentication or authorization attempts. Logged commands include those entered by users at the CLI prompt and by client applications. Authentication and authorization attempts include events that are saved in the file named `cli-commands` and those that are sent to the terminal of a user who is logged in.

```
[edit system]
syslog {
  file cli-commands {
    interactive-commands info;
    authorization info;
  }
  user * {
    interactive-commands info;
    authorization info;
  }
}
```

The following example shows how to log all alarms state changes to the file `/var/log/alarms`:

```
[edit system]
syslog {
  file alarms {
    kernel warning;
  }
}
```

The following example shows how to configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user alex, to a remote machine, and to the console:

```
[edit system]
syslog {
  /* write all security-related messages to file /var/log/security */
```



```

file security {
    authorization info;
    interactive-commands info;
}
/* write messages about potential problems to file /var/log/messages: */
/* messages from "authorization" facility at level "notice" and above, */
/* messages from all other facilities at level "warning" and above */
file messages {
    authorization notice;
    any warning;
}
/* write all messages at level "critical" and above to terminal of user
   "alex" if */
/* that user is logged in */
user alex {
    any critical;
}
/* write all messages from the "daemon" facility at level "info" and above, and */
/* messages from all other facilities at level "warning" and above, to the
   */
/* machine monitor.mycompany.com */
host monitor.mycompany.com {
    daemon info;
    any warning;
}
/* write all messages at level "error" and above to the system console */
console {
    any error;
}
}

```

The following example shows how to configure the handling of messages generated when users issue Junos OS CLI commands, by specifying the interactive-commands facility at the info, notice, and warning severity levels:

```

[edit system]
file user-actions {
    interactive-commands info;
}
user philip {
    interactive-commands notice;
}
console {
    interactive-commands warning;
}
}

```

The following list describes the security levels used in the example:

- **info**—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file `/var/log/user-actions`.

- **notice**—Logs a message when users issue the configuration mode command **commit**. The example writes the messages to the terminal of user philip.
- **warning**—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

**Related
Documentation**

- [Overview of Single-Chassis System Logging Configuration on page 89](#)

Examples: Assigning an Alternative Facility

This topic contains examples of configuring system log messages to use an alternative facility for logging.

The following example shows how to log all messages generated on the switch at the **error** level or higher to the **local0** facility on the remote host called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

The following example contains two sets of statements that show how to configure switches located in California and in New York to send messages to a single remote host called **central-logger.mycompany.com**. The messages from California are assigned to alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- The following statements configure the California switch to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local0;
}
```

- The following statements configure the New York switch to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local2;
}
```

On the remote host named **central-logger** you can subsequently configure the system logging utility to write messages from the **local0** facility to one file (for example, **california-config**) and the messages from the **local2** facility to another file (for example, **new-york-config**).

- Related Documentation**
- [Alternate Facilities for System Log Messages Directed to a Remote Destination on page 161](#)

Example: Configuring System Log Messages

The QFabric system monitors events that occur on its component devices and distributes system log messages about those events to all external system log message servers (hosts) that are configured. Component devices may include Node devices, Interconnect devices, Director devices, and the Virtual Chassis. Messages are stored for viewing only in the QFabric system database. To view the messages, issue the **show log** command.

This example describes how to configure system log messages on the QFabric system.

- [Requirements on page 169](#)
- [Overview on page 169](#)
- [Configuration on page 169](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- QFabric system
- External servers that can be configured as system log message hosts

Overview

Component devices that generate system log message events may include Node devices, Interconnect devices, Director devices, and the control plane switches. The following configuration example includes these components in the QFabric system:

- Director software running on the Director group
- Control plane switches
- Interconnect device
- Multiple Node devices

Configuration

CLI Quick Configuration

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

```
set system syslog host 10.1.1.12 any error
set system syslog file qflogs
set system syslog file qflogs structured-data brief
set system syslog file qflogs archive size 1g
```


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

To configure system messages from the QFabric Director device:

1. Specify a host, any facility, and the **error** severity level.

```
[edit system syslog]
user@switch# set host 10.1.1.12 any error
```



NOTE: You can configure more than one system log message server (host). The QFabric system sends the messages to each server configured.

2. (Optional) Specify a filename to capture log messages.



NOTE: On the QFabric system, a syslog file named **messages** is configured implicitly with facility and severity levels of **any any** and a file size of 100 MBs. Therefore, you cannot specify the filename **messages** in your configuration, and automatic command completion does not work for that filename.

```
[edit system syslog]
user@switch# set file qflogs structured-data brief
user@switch# set file qflogs
```

3. (Optional) Configure the maximum size of your system log message archive file. This example specifies an archive size of 1 GB.

```
[edit system syslog]
user@switch# set file qflogs archive size 1g
```

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

```
[edit]
user@switch# show system
syslog {
  file qflogs {
  }
  host 10.1.1.12 {
    any error;
  }
}
```

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

- Related Documentation**
- [Understanding the Implementation of System Log Messages on the QFabric System on page 91](#)
 - [syslog \(QFabric System\) on page 375](#)
 - [show log on page 416](#)

PART 3

Monitoring and Troubleshooting

- [Routine Monitoring Using the CLI on page 175](#)
- [Troubleshooting Overview on page 191](#)
- [Troubleshooting Procedures on page 199](#)

Routine Monitoring Using the CLI

- [Displaying a Log File from a Single-Chassis System on page 175](#)
- [Monitoring Traffic Through the Router or Switch on page 176](#)
- [Monitoring RMON MIB Tables on page 179](#)
- [Monitoring SNMP on page 179](#)
- [Monitoring System Log Messages on page 181](#)
- [Pinging Hosts on page 182](#)
- [Tracing SNMP Activity on a Device Running Junos OS on page 183](#)
- [Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage on page 186](#)
- [Displaying Commit Script Output on page 188](#)

Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue the following commands:

```
user@switch> show log log-filename
user@switch> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine.

The following example shows the output from the **show log messages** command:

```
user@switch1> show log messages
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 1
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 2
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 3
...
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Management
process): new instance detected (variable: sysApp1ElmtRunMemory.5.6.2293)
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Command-line
interface): new instance detected (variable: sysApp1ElmtRunMemory.5.8.2292)
...
Nov  4 12:08:30 switch1 rpdf[957]: task_connect: task BGP_100.10.10.1.6+179 addr
```



```

10.10.1.6+179: Can't assign requested
address
Nov  4 12:08:30 switch1 rpdf[957]: bgp_connect_start: connect 10.10.1.6 (Internal
AS 100): Can't assign requested address
Nov  4 12:10:24 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'exit '
Nov  4 12:10:27 switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
configuration mode
Nov  4 12:10:31 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'show log messages

```

The following example shows the output from the **file show** command. The file in the pathname **/var/log/processes** has been previously configured to include messages from the daemon facility.

```

user@switch1> file show /var/log/processes
Feb 22 08:58:24 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 22 20:35:07 switch1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 23 07:38:19 switch1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
SNMP trap: cold start
...

```

Related Documentation

- [Interpreting Messages Generated in Standard Format on page 156](#)
- [Interpreting Messages Generated in Structured-Data Format on page 153](#)

Monitoring Traffic Through the Router or Switch

To help with the diagnosis of a problem, display real-time statistics about the traffic passing through physical interfaces on the router or switch.

To display real-time statistics about physical interfaces, perform these tasks:

1. [Displaying Real-Time Statistics About All Interfaces on the Router or Switch on page 176](#)
2. [Displaying Real-Time Statistics About an Interface on the Router or Switch on page 177](#)

Displaying Real-Time Statistics About All Interfaces on the Router or Switch

Purpose Display real-time statistics about traffic passing through all interfaces on the router or switch.

Action To display real-time statistics about traffic passing through all interfaces on the router or switch:

```
user@host> monitor interface traffic
```

Sample Output

```

user@host> monitor interface traffic
host name                Seconds:15                Time: 12:31:09
Interface    Link    Input packets    (pps)    Output packets    (pps)
so-1/0/0     Down           0          (0)           0          (0)

```


so-1/1/0	Down	0	(0)	0	(0)
so-1/1/1	Down	0	(0)	0	(0)
so-1/1/2	Down	0	(0)	0	(0)
so-1/1/3	Down	0	(0)	0	(0)
t3-1/2/0	Down	0	(0)	0	(0)
t3-1/2/1	Down	0	(0)	0	(0)
t3-1/2/2	Down	0	(0)	0	(0)
t3-1/2/3	Down	0	(0)	0	(0)
so-2/0/0	Up	211035	(1)	36778	(0)
so-2/0/1	Up	192753	(1)	36782	(0)
so-2/0/2	Up	211020	(1)	36779	(0)
so-2/0/3	Up	211029	(1)	36776	(0)
so-2/1/0	Up	189378	(1)	36349	(0)
so-2/1/1	Down	0	(0)	18747	(0)
so-2/1/2	Down	0	(0)	16078	(0)
so-2/1/3	Up	0	(0)	80338	(0)
at-2/3/0	Up	0	(0)	0	(0)
at-2/3/1	Down	0	(0)	0	(0)

Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D

Meaning The sample output displays traffic data for active interfaces and the amount that each field has changed since the command started or since the counters were cleared by using the **C** key. In this example, the **monitor interface** command has been running for 15 seconds since the command was issued or since the counters last returned to zero.

Displaying Real-Time Statistics About an Interface on the Router or Switch

Purpose Display real-time statistics about traffic passing through an interface on the router or switch.

Action To display traffic passing through an interface on the router or switch, use the following Junos OS CLI operational mode command:

```
user@host> monitor interface interface-name
```

Sample Output

```
user@host> monitor interface so-0/0/1
Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
R1
Interface: so-0/0/1, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: 0C3 Traffic statistics:
  Input bytes:          5856541 (88 bps)
  Output bytes:         6271468 (96 bps)
  Input packets:        157629 (0 pps)
  Output packets:       157024 (0 pps)
Encapsulation statistics:
  Input keepalives:     42353
  Output keepalives:    42320
  LCP state: Opened
Error statistics:
  Input errors:         0
  Input drops:          0
  Input framing errors: 0
  Input runs:           0
  Input giants:         0
  Policed discards:     0
  L3 incompletes:       0
```



```

L2 channel errors:                0
L2 mismatch timeouts:            0
Carrier transitions:              1
Output errors:                   0
Output drops:                    0
Aged packets:                    0
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                      1
  LOF count                      1
  SEF count                      1
  ES-S                          77
  SES-S                          77
SONET statistics:
  BIP-B1                        0
  BIP-B2                        0
  REI-L                        0
  BIP-B3                        0
  REI-P                        0
Received SONET overhead:  F1      : 0x00 J0      : 0xZ

```

Meaning The sample output shows the input and output packets for a particular SONET interface (**so-0/0/1**). The information can include common interface failures, such as SONET/SDH and T3 alarms, loopbacks detected, and increases in framing errors. For more information, see *Checklist for Tracking Error Conditions*.

To control the output of the command while it is running, use the keys shown in [Table 32 on page 178](#).

Table 32: Output Control Keys for the monitor interface Command

Action	Key
Display information about the next interface. The monitor interface command scrolls through the physical or logical interfaces in the same order that they are displayed by the show interfaces terse command.	N
Display information about a different interface. The command prompts you for the name of a specific interface.	I
Freeze the display, halting the display of updated statistics.	F
Thaw the display, resuming the display of updated statistics.	T
Clear (zero) the current delta counters since monitor interface was started. It does not clear the accumulative counter.	C
Stop the monitor interface command.	Q

See the [CLI Explorer](#) for details on using match conditions with the **monitor traffic** command.

Monitoring RMON MIB Tables

Purpose Monitor remote monitoring (RMON) alarm, event, and log tables.

Action To display the RMON tables:

```
user@switch> show snmp rmon
Alarm
Index  Variable description                               Value State
-----
      5  monitor
          jnxOperatingCPU.9.1.0.0                     5 falling threshold

Event
Index  Type                               Last Event
-----
      1  log and trap                     2010-07-10 11:34:17 PDT
Event Index: 1
  Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
  Time: 2010-07-10 11:34:07 PDT
  Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
  Time: 2010-07-10 11:34:17 PDT
```

Meaning The display shows that an alarm has been defined to monitor jnxRmon MIB object jnxOperatingCPU, which represents the CPU utilization of the Routing Engine. The alarm is configured to generate an event that sends an SNMP trap and adds an entry to the logTable in the RMON MIB. The log table shows that two occurrences of the event have been generated—one for rising above a threshold of 90 percent, and one for falling below a threshold of 75 percent.

Related Documentation

- [Configuring RMON Alarms and Events on page 130](#)
- [show snmp rmon on page 434](#)
- [show snmp rmon history on page 438](#)
- [clear snmp statistics on page 382](#)
- [clear snmp history on page 381](#)

Monitoring SNMP

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.

- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the **show snmp health-monitor** command:

```
user@switch> show snmp health-monitor
Alarm
Index  Variable description                               Value State

32768 Health Monitor: root file system utilization
      jnxHrStoragePercentUsed.1                      58 active

32769 Health Monitor: /config file system utilization
      jnxHrStoragePercentUsed.2                      0 active

32770 Health Monitor: RE 0 CPU utilization
      jnxOperatingCPU.9.1.0.0                        0 active

32773 Health Monitor: RE 0 Memory utilization
      jnxOperatingBuffer.9.1.0.0                    35 active

32775 Health Monitor: jkernel daemon CPU utilization
      Init daemon                                    0 active
      Chassis daemon                                50 active
      Firewall daemon                               0 active
      Interface daemon                              5 active
      SNMP daemon                                   11 active
      MIB2 daemon                                   42 active
      ...
```

The following example provides sample output from the **show snmp mib** command:

```
user@switch> show snmp mib walk system

sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.juniper.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the **show snmp statistics** command:

```
user@switch> show snmp statistics

SNMP statistics:
Input:
  Packets: 0, Bad versions: 0, Bad community names: 0,
  Bad community uses: 0, ASN parse errors: 0,
  Too big: 0, No such names: 0, Bad values: 0,
  Read only: 0, General errors: 0,
```



```

Total request varbinds: 0, Total set varbinds: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0,
Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
Throttle drops: 0, Duplicate request drops: 0
Output:
Packets: 0, Too bigs: 0, No such names: 0,
Bad values: 0, General errors: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0

```

- Related Documentation**
- [health-monitor on page 289](#)
 - [show snmp mib on page 431](#)
 - [show snmp statistics on page 439](#)

Monitoring System Log Messages

Purpose Display system log messages about the QFX Series and OCX Series. By looking through a system log file for any entries pertaining to the interface that you are interested in, you can further investigate a problem with an interface on the switch.

Action To view system log messages:

```
user@switch1> show log messages
```

Sample Output

```

Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 1
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 2
Nov  4 11:30:06 switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
for Fan 3
...
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Management process): new instance detected (variable:
sysApp1ElmtRunMemory.5.6.2293)
Nov  4 11:52:53 switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Command-line interface): new instance detected (variable:
sysApp1ElmtRunMemory.5.8.2292)
...
Nov  4 12:10:24 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'exit '
Nov  4 12:10:27 switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
configuration mode
Nov  4 12:10:31 switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
'show log messages

```

Meaning The sample output shows the following entries in the **messages** file:

- A new log file was created when the previous file reached the maximum size of 128 kilobytes (KB).
- The fan speed for Fan 1, 2, and 3 is set at 65 percent.
- Health monitoring activity is detected.
- CLI commands were entered by the user jsmith.

Related Documentation

- [Overview of Junos OS System Log Messages on page 89](#)
- [Understanding the Implementation of System Log Messages on the QFabric System on page 91](#)
- [Example: Configuring System Log Messages on page 169](#)
- `clear log`
- [show log on page 416](#)
- [syslog on page 373](#)

Pinging Hosts

Purpose Use the CLI **ping** command to verify that a host can be reached over the network. This command is useful for diagnosing host and network connectivity problems. The switch sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to a specified host and receives ICMP echo responses.

Action To use the **ping** command to send four requests (ping count) to host3:
ping host count number

Sample Output

```
ping host3 count 4
user@switch> ping host3 count 4
PING host3.site.net (176.26.232.111): 56 data bytes
64 bytes from 176.26.232.111: icmp_seq=0 ttl=122 time=0.661 ms
64 bytes from 176.26.232.111: icmp_seq=1 ttl=122 time=0.619 ms
64 bytes from 176.26.232.111: icmp_seq=2 ttl=122 time=0.621 ms
64 bytes from 176.26.232.111: icmp_seq=3 ttl=122 time=0.634 ms

--- host3.site.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

- Meaning**
- The **ping** results show the following information:
 - Size of the ping response packet (in bytes).
 - IP address of the host from which the response was sent.
 - Sequence number of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
 - Time-to-live (ttl) hop-count value of the ping response packet.

- Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
- Number of ping requests (probes) sent to the host.
- Number of ping responses received from the host.
- Packet loss percentage.
- Round-trip time statistics: minimum, average, maximum, and standard deviation of the round-trip time.

**Related
Documentation**

- [Troubleshooting Overview on page 193](#)
- [Understanding Troubleshooting Resources on page 191](#)

Tracing SNMP Activity on a Device Running Junos OS

SNMP tracing operations track activity for SNMP agents and record the information in log files. The logged error descriptions provide detailed information to help you solve problems faster.

By default, Junos OS does not trace any SNMP activity. If you include the **traceoptions** statement at the **[edit snmp]** hierarchy level, the default tracing behavior is:

- Important activities are logged in files located in the **/var/log** directory. Each log is named after the SNMP agent that generates it. Currently, the following log files are created in the **/var/log** directory when the **traceoptions** statement is used:
 - chassisd
 - craftd
 - ilmid
 - mib2d
 - rmopd
 - serviced
 - snmpd
- When a trace file named **filename** reaches its maximum size, it is renamed **filename.0**, then **filename.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)
- Log files can be accessed only by the user who configured the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
traceoptions {
```



```
file <files number> <match regular-expression> <size size> <world-readable |  
no-world-readable>;  
flag flag;  
memory-trace;  
no-remote-trace;  
no-default-memory-trace;  
}
```

These statements are described in the following sections:

- [Configuring the Number and Size of SNMP Log Files on page 184](#)
- [Configuring Access to the Log File on page 184](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 185](#)
- [Configuring the Trace Operations on page 185](#)

Configuring the Number and Size of SNMP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename.0*, then *filename.1*, and so on, until there are three trace files. Then the oldest trace file (*filename.2*) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]  
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename.0*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0* is renamed *filename.1* and *filename* is renamed *filename.0*. This process repeats until there are 20 trace files. Then the oldest file (*filename.19*) is overwritten by the newest file (*filename.0*).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configured the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]  
file world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]  
file no-world-readable;
```


Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged activities.

You can refine the output by including the **match** statement at the **[edit snmp traceoptions file *filename*]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit snmp traceoptions]
file filename match regular-expression;
```

Configuring the Trace Operations

By default, only important activities are logged. You can specify which trace operations are to be logged by including the following **flag** statement (with one or more tracing flags) at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
flag {
  all;
  configuration;
  database;
  events;
  general;
  interface-stats;
  nonvolatile-sets;
  pdu;
  policy;
  protocol-timeouts;
  routing-socket;
  server;
  subagent;
  timer;
  varbind-error;
}
```

Table 33 on page 185 describes the meaning of the SNMP tracing flags.

Table 33: SNMP Tracing Flags

Flag	Description	Default Setting
all	Log all operations.	Off
configuration	Log reading of the configuration at the [edit snmp] hierarchy level.	Off
database	Log events involving storage and retrieval in the events database.	Off
events	Log important events.	Off
general	Log general events.	Off
interface-stats	Log physical and logical interface statistics.	Off

Table 33: SNMP Tracing Flags (*continued*)

Flag	Description	Default Setting
nonvolatile-set	Log nonvolatile SNMP set request handling.	Off
pdu	Log SNMP request and response packets.	Off
policy	Log policy processing.	Off
protocol-timeouts	Log SNMP response timeouts.	Off
routing-socket	Log routing socket calls.	Off
server	Log communication with processes that are generating events.	Off
subagent	Log subagent restarts.	Off
timer	Log internal timer events.	Off
varbind-error	Log variable binding errors.	Off

To display the end of the log for an agent, issue the **show log agentd | last** operational mode command:

```
[edit]
user@host# run show log agentd | last
```

where **agent** is the name of an SNMP agent.

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level](#)
- [Example: Tracing SNMP Activity](#)
- [Configuring SNMP on page 121](#)

Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage

Even though the Junos OS has built-in performance metrics and monitoring options, you might need to have customized performance metrics. To make it easier for you to monitor such customized data through a standard monitoring system, the Junos OS provides you with an enterprise-specific Utility MIB that can store such data and thus extend SNMP support for managing and monitoring the data of your choice.

The enterprise-specific Utility MIB provides you with container objects of the following types: **32-bit counters**, **64-bit counters**, **signed integers**, **unsigned integers**, and **octet strings**. You can use these container MIB objects to store the data that are otherwise not supported for SNMP operations. You can populate data for these objects either by using

CLI commands or with the help of Op scripts and an RPC API that can invoke the CLI commands.

The following CLI commands enable you to set and clear Utility MIB object values:

- **request snmp utility-mib set** instance *name* object-type <counter | counter 64 | integer | string | unsigned integer> object-value *value*
- **request snmp utility-mib clear** instance *name* object-type <counter | counter 64 | integer | string | unsigned integer>

The **instance *name*** option of the **request snmp utility-mib <set | clear>** command specifies the name of the data instance and is the main identifier of the data. The **object-type <counter | counter 64 | integer | string | unsigned integer>** option enables you specify the object type, and the **object-value *value*** option enables you to set the value of the object.

To automate the process of populating Utility MIB data, you can use a combination of an event policy and event script. The following examples show the configuration for an event policy to run **show system buffers** every hour and to store the **show system buffers** data in Utility MIB objects by running an event script (**check-mbufs.slax**).

Event Policy Configuration

To configure an event policy that runs the **show system buffers** command every hour and invokes **check-mbufs.slax** to store the **show system buffers** data into Utility MIB objects, include the following statements at the **[edit]** hierarchy level:

```
event-options {
  generate-event {
    1-HOUR time-interval 3600;
  }
  policy Mbufs {
    events 1-HOUR;
    then {
      event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
    }
  }
  event-script {
    file check-mbufs.slax;
  }
}
```

check-mbufs.slax Script

The following example shows the **check-mbufs.slax** script that is stored under **/var/db/scripts/event/**:

```
----- script START -----
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
  <op-script-results>{
    var $cmd = <command> "show system buffers";
    var $out = jcs:invoke($cmd);
```



```

var $lines = jcs:break_lines($out);
for-each ($lines) {
    if (contains(., "current/peak/max")) {
        var $pattern = "([0-9]+)/([0-9]+)/([0-9]+) mbufs";
        var $split = jcs:regex($pattern, .);
        var $result = $split[2];

        var $rpc = <request-snmp-utility-mib-set> {
            <object-type> "integer";
            <instance> "current-mbufs";
            <object-value> $result;
        }
        var $res = jcs:invoke($rpc);
    }
}
}
----- script END -----

```

You can run the following command to check the data stored in the Utility MIB as a result of the event policy and script shown in the preceding examples:

```

user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs"
= 0 jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c 03 14 2c 00 2d 07 00
regress@caramels>

```



NOTE: The `show snmp mib walk` command is not available on the QFabric system, but you can use external SNMP client applications to perform this operation.

Related Documentation

- [Understanding the Implementation of SNMP on the QFabric System on page 42](#)

Displaying Commit Script Output

Table 34 on page 188 summarizes the Junos OS command-line interface (CLI) commands you can use to monitor and troubleshoot commit scripts. For more information about the `cscript.log` file, see *Tracing Commit Script Processing*.



NOTE: Tracing commit script processing, including the `cscript.log` file, is not supported on the QFX3000-G QFabric system.

Table 34: Commit Script Configuration and Operational Mode Commands

Task	Command
Configuration Mode Commands	
Display errors and warnings generated by commit scripts.	<code>commit</code> or <code>commit check</code>
Display detailed information.	<code>commit display detail</code>

Table 34: Commit Script Configuration and Operational Mode Commands (*continued*)

Task	Command
Display the underlying Extensible Markup Language (XML) data.	commit display xml
Display the postinheritance contents of the configuration database. This view includes transient changes, but does not include changes made in configuration groups.	show display commit-scripts
Display the postinheritance contents of the configuration database. This view excludes transient changes.	show display commit-scripts no-transients
Display the postinheritance configuration in XML format. Viewing the configuration in XML format can be helpful when you are writing XML Path Language (XPath) expressions and configuration element tags.	show display commit-scripts view
Display the postinheritance configuration in XML format, but exclude transient changes.	show display commit-scripts view display commit-scripts no-transients
Display all configuration groups data, including script-generated changes to the groups.	show groups display commit-scripts
Display a particular configuration group, including script-generated changes to the group.	show groups <i>group-name</i> display commit-scripts
Operational Mode Commands	
Display logging data associated with all commit script processing.	show log cscript.log
Display processing for only the most recent commit operation.	show log cscript.log last
Display processing for script errors.	show log cscript.log match error
Display processing for a particular script.	show log cscript.log match <i>filename</i>

Related Documentation

- *Tracing Commit Script Processing*

CHAPTER 15

Troubleshooting Overview

- [Understanding Troubleshooting Resources on page 191](#)
- [Troubleshooting Overview on page 193](#)
- [Automation Enhancements Frequently Asked Questions on page 195](#)

Understanding Troubleshooting Resources

This topic describes some of the troubleshooting resources available for the QFX Series or OCX Series. These resources include tools such as the Junos OS CLI, Junos Space applications, and the Advanced Insight Scripts (AI-Scripts).

[Table 35 on page 191](#) provides a list of some of the troubleshooting resources.

Table 35: Troubleshooting Resources on the QFX and OCX Series

Troubleshooting Resource	Description	Documentation
Chassis alarms	Chassis alarms indicate a failure on the switch or one of its components. A chassis alarm count is displayed on the LCD panel on the front of the switch.	<i>Chassis Alarm Messages on a QFX3500 Device</i>
Chassis Status LEDs and Fan Tray LEDs	A blinking amber Power, Fan, or Fan Tray LED indicates a hardware component error. A blinking amber Status LED indicates a software error.	<i>Chassis Status LEDs on a QFX3500 Device</i>
Interface alarms	A predefined alarm (red or yellow) for an interface type is triggered when an interface of that type goes down.	<i>Interface Alarm Messages</i>
System alarms	A predefined alarm is triggered by a missing rescue configuration or problem with the software license.	<i>Understanding Alarms</i>
System log messages	The system log includes details of system and user events, including errors. Specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	<ul style="list-style-type: none">• Overview of Single-Chassis System Logging Configuration on page 89• Junos OS System Log Configuration Statements on page 144

Table 35: Troubleshooting Resources on the QFX and OCX Series (*continued*)

Troubleshooting Resource	Description	Documentation
Junos OS operational mode commands	Operational mode commands can be used to monitor switch performance and current activity on the network. For example, use the traceroute monitor command to locate points of failure in a network.	<ul style="list-style-type: none"> • Monitoring System Process Information • Monitoring System Properties • traceroute monitor
Junos OS automation scripts (event scripts)	Event scripts can be used to automate network troubleshooting and management tasks.	Junos OS Automation Library
Junos OS XML operational tags	XML operational tags are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device.	Junos XML API Operational Developer Reference
NETCONF XML management protocol	The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as show , set , and commit to perform those operations.	NETCONF XML Management Protocol Developer Guide
SNMP MIBs and traps	MIBs enable the monitoring of network devices from a central location. For example, use the Traceroute MIB to monitor devices remotely.	<ul style="list-style-type: none"> • SNMP MIBs Support on page 56 • SNMP Traps Support on page 72 • Using the Traceroute MIB for SNMP Remote Operations
AI-Scripts and Advanced Insight Manager (AIM)	AI-Scripts installed on the switch can automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems and submit problem reports to Juniper Support Systems.	Advanced Insight Scripts (AI-Scripts) Release Notes
Junos Space Service Now	This application enables you to display and manage information about problem events. When problems are detected on the switch by Advanced Insight Scripts (AI-Scripts) that are installed on the switch, the data is collected and sent to Service Now for your review and action.	Service Automation

Table 35: Troubleshooting Resources on the QFX and OCX Series (*continued*)

Troubleshooting Resource	Description	Documentation
Junos Space Service Insight	This application helps in accelerating operational analysis and managing the exposure to known issues. You can identify devices that are nearing their End Of Life (EOL) and also discover and prevent issues that could occur in your network. The functionality of Service Insight is dependent on the information sent from Service Now.	<i>Service Automation</i>
Juniper Networks Knowledge Base	You can search in this database for Juniper Networks product information, including alerts and troubleshooting tips.	http://kb.juniper.net

Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you may encounter on your QFX Series or OCX Series product.

[Table 36 on page 193](#) provides a list of problem categories, summary of the symptom or problem, and recommended actions with links to the troubleshooting documentation.

Table 36: Troubleshooting on the QFX Series

Problem Category	Symptom or Problem	Recommended Action
Switch hardware components	LCD panel shows a chassis alarm count.	<i>See Chassis Alarm Messages on a QFX3500 Device.</i>
	Fan tray LED is blinking amber.	<i>See Fan Tray LED on a QFX3500 Device.</i>
	Chassis status LED for the power is blinking amber.	<i>See Chassis Status LEDs on a QFX3500 Device.</i>
	Chassis status LED for the fan (on the management board) is blinking amber.	Replace the management board as soon as possible. <i>See Chassis Status LEDs on a QFX3500 Device.</i>

Table 36: Troubleshooting on the QFX Series (*continued*)

Problem Category	Symptom or Problem	Recommended Action
Port configuration	Cannot configure a port as a Gigabit Ethernet port.	<p>Check whether the port is a valid Gigabit Ethernet port (6 through 41).</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a port as a Fibre Channel port.	<p>Check whether the port is a valid Fibre Channel port (0 through 5 and 42 through 47).</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a port as a 10-Gigabit Ethernet port.	<p>If the port is not a 40-Gbps QSFP+ interface, check whether the port is in the range of 0 through 5 or 42 through 47. If one of the ports in that block (0 through 5 or 42 through 47) is configured as a Fibre Channel port, then all ports in that block must also be configured as Fibre Channel ports.</p> <p>If the port is a 40-Gbps QSFP+ interface, make sure the configuration does not exceed the interface limit. Each 40-Gbps QSFP+ interface can be split into four 10-Gigabit Ethernet interfaces, but because port 0 is reserved, so you can only configure an additional fifteen 10-Gigabit Ethernet interfaces.</p> <p>See <i>QFX3500 Device Overview</i>.</p>
	Cannot configure a 40-Gbps QSFP+ interface.	<p>The 40-Gbps QSFP+ interfaces can only be used as 10-Gigabit Ethernet interfaces. Each 40-Gbps QSFP+ interface can be split into four 10-Gigabit Ethernet interfaces using a breakout cable. However, port 0 is reserved, so you can only configure an additional fifteen 10-Gigabit Ethernet interfaces.</p> <p>See <i>QFX3500 Device Overview</i>.</p>
External devices (USB devices)	Upgrading software from a USB device results in an upgrade failure, and the system enters an invalid state.	Unplug the USB device and reboot the switch.
Initial device configuration	Cannot configure management Ethernet ports.	<p>Configure the management ports from the console port. You cannot configure the management ports by directly connecting to them.</p> <p>NOTE: The management ports are on the front panel of the QFX3500 switch. They are labeled C0 and C1 on the front panel. In the CLI they are referred to as me0 and me1.</p> <p>See <i>Configuring a QFX3500 Device as a Standalone Switch</i>.</p>

Table 36: Troubleshooting on the QFX Series (*continued*)

Problem Category	Symptom or Problem	Recommended Action
Software upgrade and configuration	Failed software upgrade.	See “Recovering from a Failed Software Installation” on page 199 .
	Active partition becomes inactive after upgrade.	
	Problem with the active configuration file.	See the following topics: <ul style="list-style-type: none"> • Loading a Previous Configuration File on page 201 • Reverting to the Default Factory Configuration on page 201 • Reverting to the Rescue Configuration on page 202 • Performing a Recovery Installation
	Root password is lost or forgotten.	Recover the root password. See “Recovering the Root Password” on page 202 .
Network interfaces	An aggregated Ethernet interface is down.	See Troubleshooting an Aggregated Ethernet Interface .
	Interface on built-in network port is down.	See Troubleshooting Network Interfaces .
	Interface on port in which SFP or SFP+ transceiver is installed in an SFP+ uplink module is down.	
Ethernet switching	A MAC address entry in the Ethernet switching table is not updated after the device with that MAC address has been moved from one interface to another on the switch.	See Troubleshooting Ethernet Switching .
Firewall filter	Firewall configuration exceeded available Ternary Content Addressable Memory (TCAM) space.	See Troubleshooting Firewall Filter Configuration .

Automation Enhancements Frequently Asked Questions

This FAQ addresses questions regarding using automation enhancements, which were introduced at Junos OS Release 13.2X51-D15 .

This FAQ covers the following questions:

- [Who Should You Contact If You Have Problems with Loading, Installing or Updating Libraries? on page 196](#)
- [Who Should You Contact If You Have Problems with Puppet for Junos OS? on page 196](#)
- [Who Should You Contact If You Have Problems with Chef for Junos OS? on page 196](#)
- [What Happens to the User Partition If You Downgrade a Device That Is Running the Junos Automation Enhancements Software Bundle to a Device That Is Running a Different Software Bundle? on page 196](#)
- [How Do You Recover Junos OS Binaries That You Have Deleted? on page 196](#)

- [How Do You Recover from a System Crash?](#) on page 196
- [How Can You Verify That a Device Is Running a Junos Automation Enhancements Software Bundle?](#) on page 196

Who Should You Contact If You Have Problems with Loading, Installing or Updating Libraries?

Contact Customer Support at <http://www.juniper.net/support>.

Who Should You Contact If You Have Problems with Puppet for Junos OS?

You can obtain support for Puppet for Junos OS through the J-Net Forum for Puppet at http://forums.juniper.net/t5/Puppet-for-Junos-OS/bd-p/puppet_junos.

Who Should You Contact If You Have Problems with Chef for Junos OS?

You can obtain support for Chef for Junos OS through the J-Net Forum for Chef at http://forums.juniper.net/t5/Chef-for-Junos-OS/bd-p/chef_junos.

What Happens to the User Partition If You Downgrade a Device That Is Running the Junos Automation Enhancements Software Bundle to a Device That Is Running a Different Software Bundle?

In this case, the user partition remains intact.



NOTE: If you make changes to the user partition while performing a unified in-service software upgrade (unified ISSU), the changes might be lost.

How Do You Recover Junos OS Binaries That You Have Deleted?

You must reinstall the software package.

How Do You Recover from a System Crash?

You must reinstall the software package.

How Can You Verify That a Device Is Running a Junos Automation Enhancements Software Bundle?

You cannot use the **show version** command to verify that a device is running the Junos Automation Enhancements software bundle. However, there are two other ways to verify this.

- On a QFX 5100 switch, use the **show configuration** command to check that you are running a Layer 3 configuration. See *Installing Junos OS Software with Junos Automation Enhancements*.
- Go to the shell and confirm that you can invoke Python. See *Invoking the Python Interpreter*.

Related Documentation

- *Overview of Junos Automation Enhancements*
- *Installing Junos OS Software with Junos Automation Enhancements*

- *Invoking the Python Interpreter*
- [Chef for Junos Getting Started Guide](#)
- [Puppet for Junos OS Documentation](#)

Troubleshooting Procedures

- [Recovering from a Failed Software Installation on page 199](#)
- [Loading a Previous Configuration File on page 201](#)
- [Reverting to the Default Factory Configuration on page 201](#)
- [Reverting to the Rescue Configuration on page 202](#)
- [Recovering the Root Password on page 202](#)
- [Troubleshooting a Deprecated Network Analytics Configuration on page 204](#)

Recovering from a Failed Software Installation

Problem **Description:** If the Junos OS appears to have been installed but the CLI does not work, or if the switch has no software installed, you can use this recovery installation procedure to install the Junos OS.

Solution If a Junos OS image already exists on the switch, you can either install the new Junos OS package in a separate partition, in which case both Junos OS images remain on the switch, or you can remove the existing Junos OS image before you start the new installation process.



NOTE: QFX5100, EX4600, and OCX Series switches do not have a separate partition to reinstall a Junos OS image.

A recovery image is created automatically on these switches. If a previously-running switch is powered on and unable to boot using a Junos OS image, you can boot the switch using the recovery Junos OS image by selecting an option in the “Select a recovery image” menu.

We suggest creating a system snapshot on your switch onto the external USB flash drive, and using the snapshot for recovery purposes. The system snapshot feature takes a “snapshot” of the files currently used to run the device—the complete contents of the /config directories, which include the running Juniper Networks Junos OS, the active configuration, and the rescue configuration, as well as the host OS—and copies all of these files into an external USB flash drive. See *Creating a Snapshot and Using It to Boot a QFX Series Switch* or *Creating a Snapshot and Using It to Boot a Device*.

To perform a recovery installation:

1. Power on the switch. The loader script starts.
2. After the message **Loading /boot/defaults/loader.conf** appears, you are prompted with the following message:

Hit [Enter] to boot immediately, or space bar for command prompt.

Press the Spacebar to enter the manual loader. The **loader>** prompt appears.



NOTE: The loader prompt does not appear on QFX5100, EX4600, and OCX Series switches.

On QFX5100, EX4600, and OCX Series switches only, a recovery image is automatically saved if a previously-running switch is powered on and unable to boot using a Junos OS image.

The “Select a recovery image” menu appears on the console when one of these switches is booted and unable to load a version of Junos OS. Follow the instructions in the “Select a recovery image” menu to load the recovery version of Junos OS for one of these switches.

You can ignore the remainder of this procedure if you are using a QFX5100, EX4600, or OCX Series switch.

3. Enter the following command:

```
loader> install [– –format] [– –external] source
```

where:

- **format**—Enables you to erase the installation media before installing the installation package. If you do not include this option, the system installs the new Junos OS in a different partition from that of the most recently installed Junos OS.
- **external**—Installs the installation package onto external media (a USB stick, for example).
- **source**—Represents the name and location of the Junos OS package, either on a server on the network or as a file on an external media, as shown in the following two examples:
 - Network address of the server and the path on the server; for example, **tftp://192.171.28/junos/jinstall-qfx-11.1R1.5-domestic-signed.tgz**
 - Junos OS package on a USB device (commonly stored in the root drive as the only file), for example, **file:///jinstall-qfx-11.1R1.5-domestic-signed.tgz**.

The installation now proceeds normally and ends with a login prompt.

Related Documentation

- *Creating a Snapshot and Using It to Boot a QFX Series Switch*

- *Creating a Snapshot and Using It to Boot a Device*

Loading a Previous Configuration File

You can use the **rollback <number>** command to return to a previously committed configuration file. A switch saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the **commit** configuration command.

Syntax

rollback <number>

Options

- **none**—Return to the most recently saved configuration.
- **number**—Return to the specified configuration.
 - **Range:** 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49.
 - **Default:** 0

To return to a configuration prior to the most recently committed one:

1. Specify the rollback number (here, 1 is entered and the configuration returns to the previously committed configuration 0):

```
[edit]
user@switch# rollback 1
load complete
```

2. Activate the configuration you have loaded:

```
[edit]
user@switch# commit
```

Related Documentation

- *Configuration File Terms*

Reverting to the Default Factory Configuration

If for any reason the current active configuration fails, you can revert to the default factory configuration. The default factory configuration contains the basic configuration settings. This is the first configuration of the switch, and it is loaded when the switch is first installed and powered on.

The **load factory default** command is a standard Junos OS configuration command. This configuration command replaces the current active configuration with the default factory configuration.

To revert the switch to the rescue configuration:

1.

```
[edit]
user@switch# load factory-default
[edit]
user@switch# delete system commit factory-settings
[edit]
user@switch# commit
```

**Related
Documentation**

- *Understanding Configuration Files*
- [Loading a Previous Configuration File on page 201](#)
- [Reverting to the Rescue Configuration on page 202](#)

Reverting to the Rescue Configuration

If someone inadvertently commits a configuration that denies management access to a device and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration. The rescue configuration is a previously committed, valid configuration.

To revert the switch to the rescue configuration:

1. Enter the **load override** command.

```
[edit]
user@switch# load override filename
```
2. Commit your changes.

```
[edit]
user@switch# commit filename
```

**Related
Documentation**

- *Setting or Deleting the Rescue Configuration*
- [Reverting to the Default Factory Configuration on page 201](#)
- *Configuration File Terms*

Recovering the Root Password

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



NOTE: The root password cannot be recovered on a QFabric system.



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

To recover the root password:

1. Power off the switch by switching off the AC power outlet of the device or, if necessary, by pulling the power cords out of the device's power supplies.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the device into the RJ-45-to-DB-9 serial port adapter supplied with the device.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the device.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
8. Configure the port settings as follows:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
9. Power on the device by (if necessary) plugging the power cords into the device's power supply, or turning on the power to the device by switching on the AC power outlet the device is plugged into.

The terminal emulation screen on your management device displays the device's boot sequence.

10. When the following prompt appears, press the Spacebar to access the device's bootstrap loader command prompt:


```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
```
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.


```
ok boot -s
```
12. At the following prompt, enter **recovery** to start the root password recovery procedure.


```
Enter full pathname of shell or 'recovery' for root password recovery or RETURN
for /bin/sh: recovery
```
13. Enter configuration mode in the CLI.
14. Set the root password. For example:


```
user@switch# set system root-authentication plain-text-password
```
15. At the following prompt, enter the new root password. For example:


```
New password: juniper1
Retype new password:
```


16. At the second prompt, reenter the new root password.
17. After you have finished configuring the password, commit the configuration.

```
root@host# commit
commit complete
```

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter **y** to reboot the device.

```
Reboot the system? [y/n] y
```

Related Documentation

- *Configuring the Root Password*

Troubleshooting a Deprecated Network Analytics Configuration

Problem **Description:** After a software upgrade to Junos OS Release 13.2X51-D15 from an earlier release, the network analytics configuration is no longer valid and the feature is disabled.

Symptoms: The network analytics configuration used in Junos OS Release 13.2X51-D10 has been deprecated in Release 13.2X51-D15. Issuing the **show services analytics** command results in the following output:

```
root@qfx5100# show services analytics

queue-statistics { ## Warning: 'queue-statistics' is deprecated
    interval 1;
}
```

Cause Junos OS Release 13.2X51-D15 added enhancements to the network analytics feature, resulting in significant changes in the CLI. The updated **[edit services analytics]** hierarchy level contains some statements that have replaced those that were previously released. As a result, the earlier configuration does not work in the new release.

Solution Use the new CLI statements to reconfigure the network analytics feature.

Related Documentation

- *Network Analytics Overview*
- *analytics*

PART 4

Configuration Statements and Operational Commands

- [Configuration Statements for Network Management on page 207](#)
- [Configuration Statements for Automation Scripts on page 215](#)
- [Configuration Statements for Fabric OAM on page 235](#)
- [Configuration Statements for sFlow Technology on page 249](#)
- [Configuration Statements for SNMP on page 259](#)
- [Configuration Statements for System Log Messages on page 357](#)
- [Monitoring Commands on page 379](#)

CHAPTER 17

Configuration Statements for Network Management

- [connection-limit on page 208](#)
- [destination-override on page 209](#)
- [no-remote-trace on page 209](#)
- [protocol-version on page 210](#)
- [rate-limit on page 211](#)
- [ssh on page 212](#)
- [telnet on page 213](#)
- [tracing on page 214](#)

connection-limit

Syntax	<code>connection-limit <i>limit</i>;</code>
Hierarchy Level	<code>[edit system services finger],</code> <code>[edit system services ftp],</code> <code>[edit system services netconf ssh],</code> <code>[edit system services ssh],</code> <code>[edit system services telnet],</code> <code>[edit system services xnm-clear-text],</code> <code>[edit system services xnm-ssl]</code>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).
Options	<p>limit—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).</p> <p>Range: 1 through 250</p> <p>Default: 75</p>



NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured `connection-limit` value if the system resources are limited.

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

Related Documentation	<ul style="list-style-type: none"> • Configuring clear-text or SSL Service for Junos XML Protocol Client Applications • Configuring DTCP-over-SSH Service for the Flow-Tap Application • Configuring Finger Service for Remote Access to the Router • Configuring FTP Service for Remote Access to the Router or Switch • Configuring SSH Service for Remote Access to the Router or Switch on page 96 • Configuring Telnet Service for Remote Access to a Router or Switch
------------------------------	---

destination-override

Syntax	destination-override { syslog host <i>ip-address</i> ; }
Hierarchy Level	[edit system tracing]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Override the system-wide configuration of the switch at the [edit system tracing] hierarchy level. This statement has no effect if system tracing is not configured.
Options	syslog —System process log files to send to the remote tracing host. <ul style="list-style-type: none"> • syslog—System process log files to send to the remote tracing host. • host <i>ip-address</i>—IP address to which to send tracing information.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Tracing and Logging Operations on page 7 • tracing on page 214

no-remote-trace

Syntax	no-remote-trace
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the switch to disable remote tracing after remote tracing has been enabled.
Default	Remote tracing is disabled.
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"> • tracing on page 214

protocol-version

Syntax	<code>protocol-version <i>version</i>;</code>
Hierarchy Level	[edit system services ssh]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the secure shell (SSH) protocol version.
Default	v2 —SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.
Options	<i>version</i> —SSH protocol version: v1 , v2 , or both.
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 the SSH Protocol Version on page 97

rate-limit

Syntax	<code>rate-limit <i>limit</i>;</code>
Hierarchy Level	<code>[edit system services finger],</code> <code>[edit system services ftp],</code> <code>[edit system services netconf ssh],</code> <code>[edit system services ssh],</code> <code>[edit system services telnet],</code> <code>[edit system services xnm-clear-text],</code> <code>[edit system services xnm-ssl]</code>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.
Default	150 connections
Options	<p>rate-limit <i>limit</i>—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).</p> <p>Range: 1 through 250</p> <p>Default: 150</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"> <i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i>


ssh

Syntax	<pre>ssh { ciphers [<i>cipher-1 cipher-2 cipher-3 ...</i>]; client-alive-count-max <i>seconds</i>; client-alive-interval <i>seconds</i>; connection-limit <i>limit</i>; hostkey-algorithm <<i>algorithm</i> no-<i>algorithm</i>>; key-exchange <<i>algorithm</i>>; macs <<i>algorithm</i>>; max-sessions-per-connection <<i>number</i>>; no-passwords; no-tcp-forwarding; protocol-version [<i>v1 v2</i>]; rate-limit <i>limit</i>; root-login (<i>allow</i> <i>deny</i> <i>deny-password</i>); }</pre>
Hierarchy Level	[edit system services]
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> <p>client-alive-interval and client-alive-max-count statements introduced in Junos OS Release 12.2.</p> <p>no-passwords statement introduced in Junos OS Release 13.3.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Allow SSH requests from remote systems to the local router or switch.</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">• Configuring SSH Service for Remote Access to the Router or Switch on page 96

telnet

Syntax	<pre>telnet { connection-limit limit; rate-limit limit; }</pre>
Hierarchy Level	[edit system services]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Provide Telnet connections from remote systems to the local router or switch. The remaining statements are explained separately.
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">• <i>Configuring Telnet Service for Remote Access to a Router or Switch</i>

tracing

Syntax	<pre>tracing { destination-override syslog host <i>ip-address</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the switch to enable remote tracing to a specified host IP address.
<hr/>	
<div> NOTE: The tracing statement is not supported on the QFX3000 QFabric system.</div> <hr/>	
The following processes are supported:	
<ul style="list-style-type: none">• chassisd—Chassis-control process• eventd—Event-processing process• cosd—Class-of-service process	
If you enabled remote tracing but wish to disable it for specific processes on the switch, use the no-remote-trace statement at the [edit system <i>process-name</i> traceoptions] hierarchy level.	
Default	Remote tracing is disabled by default.
Options	destination-override syslog host <i>ip-address</i> —Overrides the global configuration for system tracing and has no effect if the tracing statement is not configured.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Tracing and Logging Operations on page 7• destination-override on page 209

CHAPTER 18

Configuration Statements for Automation Scripts

- [allow-transients on page 216](#)
- [apply-macro on page 217](#)
- [checksum on page 218](#)
- [command on page 219](#)
- [commit on page 220](#)
- [description on page 221](#)
- [direct-access on page 221](#)
- [file \(Commit Scripts\) on page 222](#)
- [file \(Op Scripts\) on page 223](#)
- [no-allow-url on page 224](#)
- [op on page 225](#)
- [optional on page 226](#)
- [refresh \(Commit Scripts\) on page 227](#)
- [refresh \(Op Scripts\) on page 228](#)
- [refresh-from \(Commit Scripts\) on page 229](#)
- [refresh-from \(Op Scripts\) on page 230](#)
- [scripts on page 231](#)
- [source \(Commit Scripts\) on page 233](#)
- [source \(Op Scripts\) on page 234](#)

allow-transients

Syntax	allow-transients;
Hierarchy Level	[edit system scripts commit]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts, enable transient configuration changes to be committed.
Default	Transient changes are disabled by default. If you do not include the allow-transients statement, and an enabled script generates transient changes, the command-line interface (CLI) generates an error message and the commit operation fails.
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Generating a Persistent or Transient Change</i>• <i>Creating a Macro to Read the Custom Syntax and Generate Related Configuration Statements</i>

apply-macro

Syntax	<pre>apply-macro <i>apply-macro-name</i> { <i>parameter-name parameter-value</i>; }</pre>
Hierarchy Level	All hierarchy levels
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 12.2 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>With commit script macros, use custom syntax in your configuration.</p> <p>Macros work by locating apply-macro statements that you include in the candidate configuration and using the values specified in the apply-macro statement as parameters to a set of instructions (the macro) defined in a commit script. The commit script alters your configuration from one that contains custom syntax into a full configuration containing standard Junos OS statements.</p> <p>In effect, your custom configuration syntax serves a dual purpose. The syntax allows you to simplify your configuration tasks, and it provides data (or <i>hooks</i>) that are used by commit script macros.</p> <p>You can include the apply-macro statement at any level of the configuration hierarchy. You can include multiple apply-macro statements at each level of the configuration hierarchy; however, each must have a unique name.</p>
Options	<p><i>apply-macro-name</i>—Name of the apply-macro statement.</p> <p><i>parameter-name</i>—One or more parameters. Parameters can be any text you want to include in your configuration.</p> <p><i>parameter-value</i>—A value that corresponds to the parameter name. Parameter values can be any text you want to include in your configuration.</p>
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none"> • <i>Overview of Creating Custom Configuration Syntax with Macros</i>

checksum

Syntax	<code>checksum (md5 sha-256 sha1) hash;</code>
Hierarchy Level	[edit event-options event-script file <i>filename</i>], [edit system scripts commit file <i>filename</i>], [edit system scripts op file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 9.5. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts and op scripts, specify the MD5, SHA-1, or SHA-256 checksum hash. When it executes a local event, commit, or op script, Junos OS verifies the authenticity of the script by using the configured checksum hash.
Options	md5 hash —MD5 checksum of this script. sha-256 hash —SHA-256 checksum of this script. sha1 hash —SHA-1 checksum of this script.
Required Privilege Level	maintenance —To view this statement in the configuration. maintenance-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Checksum Hashes for a Commit Script</i>• <i>Configuring Checksum Hashes for an Event Script</i>• <i>Configuring Checksum Hashes for an Op Script</i>• <i>Executing an Op Script from a Remote Site</i>• <i>file checksum md5</i> command in the <i>System Basics and Services Command Reference</i>• <i>file checksum sha-256</i> command in the <i>System Basics and Services Command Reference</i>• <i>file checksum sha1</i> command in the <i>System Basics and Services Command Reference</i>

command

Syntax	<code>command <i>filename-alias</i>;</code>
Hierarchy Level	[edit system scripts op file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS op scripts, configure a filename alias for the script file. This allows you to run the script by referencing either the script filename or the filename alias.
Options	<i>filename-alias</i> —Alias for the script file.
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Enabling an Op Script and Defining a Script Alias</i>

commit

Syntax `commit {
 allow-transients;
 dampen {
 dampen-options {
 cpu-factor cpu-factor;
 line-interval line-interval;
 time-interval time-interval;
 }
 }
 direct-access;
 file filename {
 checksum (md5 | sha-256 | sha1) hash;
 optional;
 refresh;
 refresh-from url;
 source url;
 }
 max-datasize
 refresh;
 refresh-from url;
 traceoptions {
 file <filename> <files number> <size size> <world-readable | no-world-readable>;
 flag flag;
 no-remote-trace;
 }
}`

Hierarchy Level [edit system [scripts](#)]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For Junos OS commit scripts, configure the commit-time scripting mechanism.

Options The statements are explained separately.

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

Related Documentation

- *Storing and Enabling Scripts*

description

Syntax	<code>description <i>descriptive-text</i>;</code>
Hierarchy Level	[edit system scripts op file filename] [edit system scripts op file filename arguments <i>argument-name</i>]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS op scripts, provide a help-text string that appears in the command-line interface (CLI).
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Help Text for Op Scripts</i> • <i>Declaring Arguments in Op Scripts</i> • file (Op Scripts) on page 223

direct-access

Syntax	<code>direct-access;</code>
Hierarchy Level	[edit system scripts commit]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify that commit scripts read input configurations directly from the database when inspecting these scripts for errors.
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Executing Large Commit Scripts</i>

file (Commit Scripts)

Syntax	<pre>file <i>filename</i> { checksum (md5 sha-256 sha1) <i>hash</i>; optional; refresh; refresh-from <i>url</i>; source <i>url</i>; }</pre>
Hierarchy Level	[edit system scripts commit]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts, enable a commit script that is located in the <code>/var/db/scripts/commit</code> directory.
Options	<p><i>filename</i>—Name of an Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) file containing a commit script.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>maintenance—To view this statement in the configuration.</p> <p>maintenance-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><i>Controlling Execution of Commit Scripts During Commit Operations</i>

file (Op Scripts)

Syntax	<pre> file <i>filename</i> { arguments { <i>argument-name</i> { description <i>descriptive-text</i>; } } checksum (md5 sha-256 sha1) <i>hash</i>; command <i>filename-alias</i>; dampen { dampen-options { cpu-factor <i>cpu-factor</i>; line-interval <i>line-interval</i>; time-interval <i>time-interval</i>; } } description <i>descriptive-text</i>; refresh; refresh-from <i>url</i>; source <i>url</i>; } </pre>
Hierarchy Level	[edit system scripts op]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	For Junos OS op scripts, enable an op script that is located in the <code>/var/db/scripts/op</code> directory.
Options	<p><i>filename</i>—The name of an Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) file containing an op script.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>maintenance—To view this statement in the configuration.</p> <p>maintenance-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Enabling an Op Script and Defining a Script Alias</i>

no-allow-url

Syntax	no-allow-url;
Hierarchy Level	[edit system scripts op]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS op scripts, prohibit the remote execution of scripts. When you include this configuration statement, the op url operational mode command generates an error and does not permit you to execute the op script from a remote site.
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• file (Op Scripts) on page 223• <i>Executing an Op Script from a Remote Site</i>

op

```
Syntax  op {
        file filename {
            arguments {
                argument-name {
                    description descriptive-text;
                }
            }
        }
        checksum (md5 | sha-256 | sha1) hash;
        command filename-alias;
        dampen {
            dampen-options {
                cpu-factor cpu-factor;
                line-interval line-interval;
                time-interval time-interval;
            }
        }
        description descriptive-text;
        max-datasize
        refresh;
        refresh-from url;
        source url;
    }
    no-allow-url
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level [edit system [scripts](#)]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For Junos OS op scripts, configure an operation scripting mechanism.


Options The statements are explained separately.

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

Related Documentation

- *Storing and Enabling Scripts*

optional

Syntax	optional;
Hierarchy Level	[edit system scripts commit file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts, allow a commit operation to succeed even if the script specified in the file statement is missing from the /var/db/scripts/commit directory on the device.
<div> NOTE: On the QFabric system, commit scripts are stored in the /pbdata/mgd_shared/partition-ip/var/db/scripts/commit/ directory on the Director device.</div>	
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Controlling Execution of Commit Scripts During Commit Operations</i>

refresh (Commit Scripts)

Syntax	refresh;
Hierarchy Level	[edit system scripts commit], [edit system scripts commit file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts, overwrite the local copy of all enabled commit scripts or a single enabled script located in the <code>/var/db/scripts/commit</code> directory with the copy located at the source URL, as specified in the source statement at the same hierarchy level.




NOTE: Issuing the `set refresh` command does not add the `refresh` statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.

The `set refresh` command is unique in the Junos OS CLI in that it behaves like an operational mode command and yet it can be executed from within configuration mode. All other Junos OS CLI operational mode commands can only be executed from command mode. The functionality is provided in this manner as a convenience to users developing commit scripts.


On the QFabric system, commit scripts are stored in the `/pbdata/mgd_shared/partition-ip/var/db/scripts/commit/` directory on the Director device.

Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Using a Master Source Location for a Script</i> • refresh-from (Commit Scripts) on page 229 • source (Commit Scripts) on page 233


refresh (Op Scripts)

Syntax	refresh;
Hierarchy Level	[edit system scripts op], [edit system scripts op file filename]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 11.1 on the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>For Junos OS op scripts, overwrite the local copy of all enabled op scripts or a single enabled script located in the <code>/var/db/scripts/op</code> directory with the copy located at the source URL, specified in the source statement at the same hierarchy level.</p> <p>The update operation occurs as soon as you issue the set refresh configuration mode command. Issuing the set refresh command does not add the refresh statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.</p> <div> NOTE: On the QFabric system, op scripts are stored in the <code>/pbdata/mgd_shared/partition-ip/var/db/scripts/op/</code> directory on the Director device.</div>
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Using a Master Source Location for a Script</i>• refresh-from (Op Scripts) on page 230• source (Op Scripts) on page 234

refresh-from (Commit Scripts)

Syntax	<code>refresh-from url;</code>
Hierarchy Level	[edit system scripts commit], [edit system scripts commit file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>For Junos OS commit scripts, overwrite the local copy of all enabled commit scripts or a single enabled script located in the <code>/var/db/scripts/commit</code> directory with the copy located at a URL other than the URL specified in the source statement.</p> <p>The update operation occurs as soon as you issue the set refresh-from url configuration mode command. Issuing the set refresh-from command does not add the refresh-from statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.</p>
<div>  NOTE: This statement is not supported on the QFabric system. </div>	
Options	url —The source specified as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (scp)-style remote file specification.
Required Privilege Level	maintenance—To view this statement in the configuration. maintenance-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Using an Alternate Source Location for a Script</i> • refresh (Commit Scripts) on page 227 • source (Commit Scripts) on page 233

refresh-from (Op Scripts)

Syntax	<code>refresh-from url;</code>
Hierarchy Level	[edit system scripts op], [edit system scripts op file filename]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 11.1 on the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>For Junos OS op scripts, overwrite the local copy of all enabled op scripts or a single enabled script located in the <code>/var/db/scripts/op</code> directory with the copy located at a URL other than the URL specified in the source statement.</p> <p>The update operation occurs as soon as you issue the set refresh-from url configuration mode command. Issuing the set refresh-from command does not add the refresh-from statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.</p>
<hr/> <div> NOTE: This statement is not supported on the QFabric system.</div> <hr/>	
Options	url —Source specified as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (scp)-style remote file specification.
Required Privilege Level	maintenance —To view this statement in the configuration. maintenance-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Using an Alternate Source Location for a Script</i>• refresh (Op Scripts) on page 228• source (Op Scripts) on page 234

scripts

```
Syntax  scripts {
    commit {
        allow-transients;
        dampen {
            dampen-options {
                cpu-factor cpu-factor;
                line-interval line-interval;
                time-interval time-interval;
            }
        }
    }
    direct-access;
    file filename {
        checksum (md5 | sha-256 | sha1) hash;
        optional;
        refresh;
        refresh-from url;
        source url;
    }
    max-datasize
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
load-scripts-from-flash;
op {
    file filename {
        arguments {
            argument-name {
                description descriptive-text;
            }
        }
        checksum (md5 | sha-256 | sha1) hash;
        command filename-alias;
        dampen {
            dampen-options {
                cpu-factor cpu-factor;
                line-interval line-interval;
                time-interval time-interval;
            }
        }
        description descriptive-text;
        max-datasize
        refresh;
        refresh-from url;
        source url;
    }
    no-allow-url
    refresh;
```



```
refresh-from url;
traceoptions {
  file <filename> <files number> <size size> <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
}
synchronize;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For Junos OS commit or op scripts, configure scripting mechanisms.



NOTE: The traceoptions statement is not supported on QFabric systems.


Options The statements are explained separately.

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


Related Documentation

- *Storing and Enabling Scripts*

source (Commit Scripts)

Syntax	<code>source url;</code>
Hierarchy Level	[edit system scripts commit file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS commit scripts, specify the location of the source file for an enabled script located in the <code>/var/db/scripts/commit</code> directory. When you include the refresh statement at the same hierarchy level and commit the configuration, the local copy is overwritten by the version stored at the specified URL.
<div>  <p>NOTE: On the QFabric system, commit scripts are stored in the <code>/pbdata/mgd_shared/partition-ip/var/db/scripts/op/</code> directory on the Director device.</p> </div>	
Options	url —The source specified as an HTTP URL, FTP URL, or scp-style remote file specification.
Required Privilege Level	maintenance —To view this statement in the configuration. maintenance-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Using a Master Source Location for a Script</i> • <i>Overview of Updating Scripts from a Remote Source</i> • refresh (Commit Scripts) on page 227 • refresh-from (Commit Scripts) on page 229

source (Op Scripts)

Syntax	<code>source url;</code>
Hierarchy Level	[edit system scripts op file filename]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	For Junos OS op scripts, specify the location of the source file for an enabled script located in the <code>/var/db/scripts/op</code> directory. When you include the refresh statement at the same hierarchy level, the local copy is overwritten by the version stored at the specified URL.
<div> NOTE: On the QFabric system, commit scripts are stored in the <code>/pbdata/mgd_shared/partition-ip/var/db/scripts/op/</code> directory on the Director device.</div>	
Options	url —Master source file for an op script specified as an HTTP URL, FTP URL, or scp-style remote file specification.
Required Privilege Level	maintenance —To view this statement in the configuration. maintenance-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Using a Master Source Location for a Script</i>• refresh (Op Scripts) on page 228• refresh-from (Op Scripts) on page 230

CHAPTER 19

Configuration Statements for Fabric OAM

- [ethernet-frame-size on page 236](#)
- [fabric \(OAM\) on page 237](#)
- [fabric-maintenance-associations on page 239](#)
- [fabric-maintenance-end-points on page 240](#)
- [flow-specs on page 241](#)
- [unicast-ethernet-ipv4 on page 243](#)
- [multicast-ipv4 on page 245](#)
- [multicast-vlan-flood on page 246](#)
- [unicast-ethernet on page 247](#)

ethernet-frame-size

Syntax	<code>ethernet-frame-size <i>ethernet-frame-size</i>;</code>
Hierarchy Level	[edit protocols oam fabric flow-specs <i>flow-specification-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure the Ethernet frame size in the flow specification parameters for internal fabric monitoring.
Options	<i>ethernet-frame-size</i> —Integer defining the size (in bytes) of the Ethernet frame. Range: 256 to 9116 bytes
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">• Overview of Internal Fabric Monitoring on page 29• Configuring a Fabric Maintenance Association on page 103• Configuring Flow Specifications on page 104• fabric (OAM) on page 237• ping fabric multicast-flow on page 398• ping fabric unicast-flow on page 400• traceroute fabric unicast-flow on page 446

fabric (OAM)

```

Syntax  fabric {
        fabric-maintenance-associations {
            fma-name {
                description string;
                fabric-maintenance-end-points {
                    fmep-id {
                        description string;
                        fmep-interface interface-name;
                        fmep-name name;
                    }
                }
                vlan-name vlan-name;
            }
        }
        flow-specs {
            flow-specification-name {
                ethernet-frame-size size;
                multicast-ipv4 {
                    dest-ip-multicast-group ipv4-mcast-address;
                    source-ip ipv4-address;
                }
                multicast-vlan-flood;
                unicast-ethernet {
                    destination-mac destination-mac-address destination-mac-mask
                        destination-mac-mask;
                    ethertype ethertype;
                    source-mac mac-address source-mac-mask source-mac-mask;
                }
                unicast-ethernet-ipv4 {
                    destination-ip destination-ip-address destination-ip-mask destination-ip-mask;
                    destination-l4-port destination-l4-port-number;
                    destination-mac destination-mac-address;
                    ip-proto protocol;
                    source-ip source-ip-address source-ip-mask source-ip-mask;
                    source-l4-port source-l4-port-number;
                }
            }
        }
        faboam-trace-options {
            file filename{
                files number;
                no-stamp;
                no-world-readable;
                replace;
                size size;
                world-readable;
            }
            flag {
                all;
                debug-all;
                ffping;
                generic;
            }
        }
    }

```



```
        netio;  
        packets;  
        trace-route;  
    }  
}  
}
```

Hierarchy Level [edit protocols oam]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the fabric maintenance association (FMA) and flow specification parameters for internal fabric monitoring.

The remaining statements are explained separately.

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

Related Documentation

- [Overview of Internal Fabric Monitoring on page 29](#)
- [Configuring a Fabric Maintenance Association on page 103](#)
- [Configuring Flow Specifications on page 104](#)
- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

fabric-maintenance-associations

```
Syntax fabric-maintenance-associations {
    fma-name {
        description string;
        fabric-maintenance-end-points {
            fmep-id {
                description string;
                fmep-interface interface-name;
                fmep-name name;
            }
        }
        vlan-name vlan-name;
    }
}
```

Hierarchy Level [edit protocols oam fabric]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the fabric maintenance association (FMA) parameters for internal fabric monitoring. The FMA defines a set of QFabric system interfaces (fabric maintenance endpoints [FMEPs]) that are members of a given VLAN which are used in internal fabric monitoring operations. The FMA associates the set of FMEPs with a VLAN. Configuration of the VLAN is mandatory.

The remaining statements under this hierarchy level are explained separately.

Options **description *string***—Description of the FMA.
Syntax: 1 to 128 alphanumeric characters

fma-name—Name of the FMA.
Syntax: 1 to 20 alphanumeric characters

vlan-name *vlan-name*—Name of the VLAN for which the FMA is defined.



NOTE: Configuring the VLAN option is mandatory.

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

Related Documentation

- [Overview of Internal Fabric Monitoring on page 29](#)
- [Configuring a Fabric Maintenance Association on page 103](#)
- [Configuring Flow Specifications on page 104](#)
- [fabric \(OAM\) on page 237](#)
- [ping fabric multicast-flow on page 398](#)

- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

fabric-maintenance-end-points

Syntax	<pre>fabric-maintenance-end-points { fmep-id { description <i>string</i>; fmep-interface <i>interface-name</i>; fmep-name <i>name</i>; } }</pre>
Hierarchy Level	[edit protocols oam fabric fabric-maintenance-associations <i>fma-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure the fabric maintenance association endpoint (FMEP) parameters within a fabric maintenance association (FMA). The FMA associates the FMEP with a VLAN for purposes of internal fabric monitoring.
Options	<p>description <i>string</i>—Description of the FMEP. Syntax: 1 to 128 alphanumeric characters</p> <p>fmep-id—32-bit integer that is used to identify an FMEP. Range: 1 to 64,000</p> <p>fmep-name <i>name</i>—Name of the fabric maintenance association endpoint. Syntax: 1 to 20 alphanumeric characters</p> <p>fmep-interface <i>interface-name</i>—Interface on a QFabric system Node device. Syntax: <i>node-device-name:interface-type-fpc/pic/slot.unit</i></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">• Overview of Internal Fabric Monitoring on page 29• Configuring a Fabric Maintenance Association on page 103• Configuring Flow Specifications on page 104• fabric (OAM) on page 237• ping fabric multicast-flow on page 398• ping fabric unicast-flow on page 400• traceroute fabric unicast-flow on page 446

flow-specs

```
Syntax  flow-specs {
        flow-specification-name {
            ethernet-frame-size ethernet-frame-size;
            multicast-ipv4 {
                dest-ip-multicast-group ipv4-mcast-address;
                source-ip ipv4-address;
            }
            multicast-vlan-flood;
            unicast-ethernet {
                destination-mac destination-mac-address destination-mac-mask
                    destination-mac-mask;
                ethertype ethertype;
                source-mac mac-address source-mac-mask source-mac-mask;
            }
            unicast-ethernet-ipv4 {
                destination-ip destination-ip-address destination-ip-mask destination-ip-mask;
                destination-l4-port destination-l4-port-number;
                destination-mac destination-mac-address;
                ip-proto protocol;
                source-ip source-ip-address source-ip-mask source-ip-mask;
                source-l4-port source-l4-port-number;
            }
        }
    }
```

Hierarchy Level [edit protocols oam fabric]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the fabric flow specification parameters for internal fabric monitoring. The following conditions apply:

- You must specify a protocol type for each flow specification: **unicast-ethernet**, **unicast-ethernet-ipv4**, **multicast-ipv4**, or **multicast-vlan-flood**.
- You can specify only one type for each flow specification.
- All other parameters are optional.

The remaining statements under this hierarchy level are explained separately.

Options *flow-specification-name*—Name of the flow specification.
Syntax: 1 to 20 alphanumeric characters

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

Related Documentation

- [Overview of Internal Fabric Monitoring on page 29](#)
- [Configuring a Fabric Maintenance Association on page 103](#)
- [Configuring Flow Specifications on page 104](#)

- [fabric \(OAM\) on page 237](#)
- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

unicast-ethernet-ipv4

Syntax	<pre>unicast-ethernet-ipv4 { source-ip <i>source-ip-address</i> source-ip-mask <i>source-ip-mask</i>; destination-ip <i>destination-ip-address</i> destination-ip-mask <i>destination-ip-mask</i>; ip-proto <i>protocol</i>; source-l4-port <i>source-l4-port-number</i>; destination-l4-port <i>destination-l4-port-number</i>; }</pre>
Hierarchy Level	[edit protocols oam fabric flow-specs <i>flow-specification-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure unicast parameters for the Ethernet IPv4 protocol type in the internal fabric monitoring flow specifications.
Options	<p>destination-ip <i>destination-ip-address</i>—Unicast IPv4 address of the destination fabric maintenance endpoint (FMEP) that is configured in the fabric maintenance association (FMA). Syntax: Dotted decimal notation without the prefix</p> <p>destination-l4-port <i>destination-l4-port-number</i>—L4 TCP or UDP port for the destination fabric maintenance endpoint (FMEP). Values: 2-byte decimal or hexadecimal notation</p> <p>ip-proto <i>protocol</i>—IPv4 protocol type. Values: 1-byte value in decimal or hexadecimal notation</p> <p>destination-ip-mask <i>destination-ip-mask</i>—IPv4 address range mask for the destination FMEP that is configured in the flow specification. The masked bits denote the range that needs to be generated. The other bits obtain their values from the corresponding source or destination IPv4 address parameter. The mask must be contiguous. Syntax: Dotted decimal notation without the prefix Values: Maximum of 6 contiguous masked bits, or a mask range of 64</p> <p>source-ip <i>source-ip-address</i>—Unicast IPv4 address of the source fabric maintenance endpoint (FMEP) that is configured in the fabric maintenance association (FMA). Syntax: Dotted decimal notation without the prefix</p> <p>source-l4-port <i>source-l4-port-number</i>—TCP or UDP port for the source fabric maintenance endpoint (FMEP). Values: 2-byte decimal or hexadecimal notation</p> <p>source-ip-mask <i>source-ip-mask</i>—IPv4 address range mask for the source FMEP that is configured in the flow specification.</p>

The masked bits denote the range that needs to be generated. The other bits obtain their values from the corresponding source or destination IPv4 address parameter. The mask must be contiguous.

Syntax: Dotted decimal notation without the prefix

Values: Maximum of 6 contiguous masked bits, or a mask range of 64

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">• Overview of Internal Fabric Monitoring on page 29• Configuring a Fabric Maintenance Association on page 103• Configuring Flow Specifications on page 104• fabric (OAM) on page 237• ping fabric multicast-flow on page 398• ping fabric unicast-flow on page 400• traceroute fabric unicast-flow on page 446
------------------------------	--

multicast-ipv4

Syntax	<pre>multicast-ipv4 { source-ip <i>source-ip-address</i>; dest-ip-multicast-group <i>ipv4-mcast-address</i>; }</pre>
Hierarchy Level	[edit protocols oam fabric flow-specs <i>flow-specification-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure multicast parameters for the IPv4 Ethernet protocol type in the internal fabric monitoring flow specifications.
Options	<p>dest-ip-multicast-group <i>ipv4-mcast-address</i>—IPv4 multicast group address of the destination fabric maintenance endpoint (FMEP) that is configured in the flow specification. Configuration of this parameter is mandatory.</p> <p>Syntax: Dotted decimal notation without the prefix</p> <p>source-ip <i>source-ip-address</i>—(Optional) IPv4 multicast address of the source fabric maintenance endpoint (FMEP) that is configured in the flow specification.</p> <p>Syntax: Dotted decimal notation without the prefix</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"> • Overview of Internal Fabric Monitoring on page 29 • Configuring a Fabric Maintenance Association on page 103 • Configuring Flow Specifications on page 104 • fabric (OAM) on page 237 • ping fabric multicast-flow on page 398 • ping fabric unicast-flow on page 400 • traceroute fabric unicast-flow on page 446

multicast-vlan-flood

Syntax	multicast-vlan-flood
Hierarchy Level	[edit protocols oam fabric flow-specs <i>flow-specification-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure parameters of the multicast VLAN flood protocol type in the internal fabric monitoring flow specification.
Options	There are no configuration options.
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">• Overview of Internal Fabric Monitoring on page 29• Configuring a Fabric Maintenance Association on page 103• Configuring Flow Specifications on page 104• fabric (OAM) on page 237• ping fabric multicast-flow on page 398• ping fabric unicast-flow on page 400• traceroute fabric unicast-flow on page 446

unicast-ethernet

Syntax	<pre>unicast-ethernet { destination-mac <i>destination-mac-address</i> destination-mac-mask <i>destination-mac-mask</i>; ethertype <i>ethertype</i>; source-mac <i>source-mac-address</i> source-mac-mask <i>source-mac-mask</i>; }</pre>
Hierarchy Level	[edit protocols oam fabric flow-specs <i>flow-specification-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	Configure unicast Ethernet parameters for a flow specification used in internal fabric monitoring.
Options	<p>destination-mac <i>destination-mac-address</i>—(Optional) MAC address of the destination fabric maintenance endpoint (FMEP) that is configured in the flow specification.</p> <p>destination-mac-mask <i>destination-mac-mask</i>—(Optional) MAC address range mask for the destination FMEP that is configured in the flow specification. You cannot configure the destination-mac-mask parameter unless you also configure the destination-mac parameter.</p> <p>The masked bits denote the range that needs to be generated. The other bits obtain their values from the corresponding source or destination MAC address parameter. The mask must be contiguous.</p> <p>Values: Maximum of 6 contiguous masked bits, or a mask range of 64</p> <p>ethertype <i>ethertype</i>—Valid Ethernet type other than the IPv4 Ethertype.</p> <p>Values: 2 bytes in decimal or hexadecimal notation</p> <p>source-mac <i>source-mac-address</i>—(Optional) MAC address of the source FMEP or interface that is configured in the flow specification.</p> <p>source-mac-mask <i>source-mac-mask</i>—(Optional) MAC address range mask for the source FMEP that is configured in the flow specification. You cannot configure the source-mac-mask parameter unless you also configure the source-mac parameter.</p> <p>The masked bits denote the range that needs to be generated. The other bits obtain their values from the corresponding source or destination MAC address parameter. The mask must be contiguous.</p> <p>Values: Maximum of 6 contiguous masked bits, or a mask range of 64</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"> • Overview of Internal Fabric Monitoring on page 29 • Configuring a Fabric Maintenance Association on page 103 • Configuring Flow Specifications on page 104 • fabric (OAM) on page 237

- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)
- [traceroute fabric unicast-flow on page 446](#)

CHAPTER 20

Configuration Statements for sFlow Technology

- [agent-id on page 249](#)
- [collector \(sFlow Technology\) on page 250](#)
- [interfaces \(sFlow\) on page 251](#)
- [polling-interval on page 252](#)
- [sample-rate on page 253](#)
- [sflow on page 254](#)
- [source-ip on page 255](#)
- [traceoptions \(sFlow Technology\) on page 256](#)
- [udp-port on page 257](#)

agent-id

Syntax	<code>agent-id <i>ip-address</i>;</code>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the IP address of the sFlow agent. If you do not configure the sFlow agent ID, the IP address for the agent is dynamically created using the IP address of an interface configured on the QFX Series device.
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 sFlow Technology on page 115• sflow on page 254

collector (sFlow Technology)

Syntax	<code>collector <i>ip-address</i> { udp-port <i>port-number</i>; }</code>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Configure a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the configured collector for analysis. You can configure up to four collectors on the device. You specify the IP address for each collector you configure.</p> <p>The remaining statement is explained separately.</p>
Options	<i>ip-address</i> —IP address of the collector.
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 sFlow Technology on page 115• Example: Monitoring Network Traffic Using sFlow Technology on page 116

interfaces (sFlow)

Syntax	<pre> interfaces <i>interface-name</i> { polling-interval <i>seconds</i>; sample-rate <i>number</i>; } </pre>
Hierarchy Level	[edit protocols sflow]
Release Information	<p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure sFlow network traffic monitoring on the specified interface on the device. You can configure sFlow parameters (polling interval, sample rate) with different values on different 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"> • Configuring sFlow Technology on page 115 • Example: Monitoring Network Traffic Using sFlow Technology on page 116

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 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the rate (in seconds) at which successive samples of interface statistics (counters) are taken.
Default	If no polling interval is configured for a particular interface, the device uses the global polling interval configured at the [edit protocols sflow] hierarchy level. If no global interval is configured, the device uses the default polling interval of 20 seconds.
Options	<i>seconds</i> —Number of seconds between successive samples of interface statistics. Specifying a value of 0 (zero) disables the polling. Range: 0 through 3600 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 sFlow Technology on page 115• Example: Monitoring Network Traffic Using sFlow Technology on page 116

sample-rate

Syntax	<code>sample-rate <i>number</i>;</code>
Hierarchy Level	<code>[edit protocols sflow],</code> <code>[edit protocols sflow interfaces <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the denominator (<i>number</i>) of the ratio that is the sample rate in sFlow traffic monitoring. For example, to configure a sample rate of 1 in 1000 packets, you specify a <i>number</i> of 1000.
Default	If no sample rate is configured for a particular interface, the device uses the global sample rate configured at the <code>[edit protocols sflow]</code> hierarchy level. If no global rate is configured, the device uses the default sample rate of 1 in 2000 packets.
Options	<i>number</i> —Denominator of the ratio representing the sample rate (one packet out of <i>number</i>). Range: 1 through 16,777,215
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring sFlow Technology on page 115 • Example: Monitoring Network Traffic Using sFlow Technology on page 116

sflow

Syntax	<pre> sflow { agent-id <i>ip-address</i>; collector <i>ip-address</i> { udp-port <i>port-number</i>; } interfaces <i>interface-name</i> { polling-interval <i>number</i>; sample-rate { egress <i>number</i>; ingress <i>number</i>; } } polling-interval <i>number</i>; sample-rate { egress <i>number</i>; ingress <i>number</i>; } source-ip <i>ip-address</i>; traceoptions { file <i>filename</i> <files <i>number</i>> <no-stamp> <replace> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } } </pre>
Hierarchy Level	[edit protocols]
Release Information	<p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure sFlow technology to monitor traffic continuously on specified interfaces simultaneously. sFlow data can be used to characterize network activity.</p> <p>The remaining statements are explained separately.</p>
Default	The sFlow protocol is disabled by default.
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 sFlow Technology on page 115 • Example: Monitoring Network Traffic Using sFlow Technology on page 116

source-ip

Syntax	<code>source-ip <i>ip-address</i>;</code>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the source IP address to be used for sFlow datagrams. If you do not configure a source IP address, it is dynamically created based on the IP address of an Ethernet interface configured on the QFX Series device.
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 sFlow Technology on page 115• sflow on page 254

traceoptions (sFlow Technology)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <no-stamp> <replace> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; }</pre>
Hierarchy Level	[edit protocols sflow]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define tracing operations for sFlow technology.
Default	The traceoptions feature is disabled.
Options	<p>file <i>filename</i>—Name of the file to receive the tracing operation output. Enclose the name in quotation marks. Output files are located in the <code>/var/log/</code> directory.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0. Incoming trace file data is logged in the now empty trace-file. When trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify the maximum number of files, you must also specify the maximum file size using the size option.</p> <p>Range: 2 through 1000 files Default: 1 trace file</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—Trace all sFlow monitoring events.• client-server—Trace sFlow monitoring client-server events.• configuration—Trace sFlow monitoring configuration events.• interface—Trace sFlow monitoring interface events.• rtsock—Trace routing socket code events. <p>no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.</p> <p>no-world-readable—(Optional) Prevent any user from reading the trace file.</p> <p>replace—(Optional) Replace an existing trace file if there is one.</p>

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**. Incoming trace file data is logged in the now empty **trace-file**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through the maximum file size of 4 GB

Default: 128 KB

world-readable—(Optional) Allow any user to read the trace file.

Required Privilege Level	routing and trace—To view this statement in the configuration.
	routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Overview of sFlow Technology on page 35

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 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the UDP port for a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the collector for analysis.
Default	Port 6343
Options	<i>port-number</i> —UDP port number for this collector.
Required Privilege Level	routing—To view this statement in the configuration.
	routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring sFlow Technology on page 115 • Example: Monitoring Network Traffic Using sFlow Technology on page 116

CHAPTER 21

Configuration Statements for SNMP

- [access \(SNMP\) on page 262](#)
- [address \(SNMP\) on page 262](#)
- [address-mask on page 263](#)
- [agent-address on page 263](#)
- [alarm \(SNMP RMON\) on page 264](#)
- [authentication-md5 on page 265](#)
- [authentication-none on page 266](#)
- [authentication-password on page 267](#)
- [authentication-sha on page 268](#)
- [authorization on page 269](#)
- [bucket-size on page 270](#)
- [categories on page 271](#)
- [client-list on page 271](#)
- [client-list-name on page 272](#)
- [clients on page 272](#)
- [commit-delay on page 273](#)
- [community \(SNMP\) on page 274](#)
- [community \(RMON\) on page 275](#)
- [community-name \(SNMP\) on page 276](#)
- [contact on page 277](#)
- [description \(SNMP\) on page 278](#)
- [description \(RMON\) on page 279](#)
- [destination-port \(SNMP\) on page 279](#)
- [engine-id on page 280](#)
- [event on page 281](#)
- [falling-event-index \(RMON\) on page 282](#)
- [falling-threshold \(Health Monitor\) on page 283](#)
- [falling-threshold \(RMON\) on page 284](#)

- [falling-threshold-interval](#) on page 285
- [filter-duplicates](#) on page 285
- [filter-interfaces](#) on page 286
- [group \(Associating a Security Name\)](#) on page 287
- [group \(Configuring Access Privileges\)](#) on page 288
- [health-monitor](#) on page 289
- [history](#) on page 290
- [interface \(SNMP\)](#) on page 291
- [interface \(RMON\)](#) on page 292
- [interval \(Health Monitor\)](#) on page 293
- [interval \(RMON\)](#) on page 294
- [local-engine](#) on page 295
- [location](#) on page 296
- [logical-system \(SNMP\)](#) on page 297
- [message-processing-model](#) on page 298
- [name](#) on page 298
- [nonvolatile](#) on page 299
- [notify](#) on page 300
- [notify-filter \(Applying to the Management Target\)](#) on page 301
- [notify-filter \(Configuring the Profile Name\)](#) on page 301
- [notify-view](#) on page 302
- [oid](#) on page 302
- [oid \(SNMPv3\)](#) on page 303
- [owner](#) on page 304
- [parameters](#) on page 305
- [port \(SNMP\)](#) on page 305
- [privacy-3des](#) on page 306
- [privacy-aes128](#) on page 307
- [privacy-des](#) on page 308
- [privacy-none](#) on page 309
- [privacy-password](#) on page 310
- [read-view](#) on page 311
- [remote-engine](#) on page 312
- [request-type](#) on page 313
- [retry-count \(SNMPv3\)](#) on page 314
- [rising-event-index](#) on page 315
- [rising-threshold \(Health Monitor\)](#) on page 316

- [rising-threshold \(RMON\) on page 317](#)
- [rmon on page 318](#)
- [routing-instance \(SNMP\) on page 319](#)
- [sample-type on page 320](#)
- [security-level \(Defining Access Privileges\) on page 321](#)
- [security-level \(Generating SNMP Notifications\) on page 322](#)
- [security-model \(Access Privileges\) on page 323](#)
- [security-model \(Group\) on page 324](#)
- [security-model \(SNMP Notifications\) on page 325](#)
- [security-name \(Community String\) on page 326](#)
- [security-name \(Security Group\) on page 327](#)
- [security-name \(SNMP Notifications\) on page 328](#)
- [security-to-group on page 329](#)
- [snmp on page 330](#)
- [snmp-community on page 334](#)
- [source-address \(SNMP\) on page 335](#)
- [startup-alarm on page 336](#)
- [syslog-subtag on page 337](#)
- [tag \(Configuring Notification Targets\) on page 337](#)
- [tag \(Configuring the SNMP Community\) on page 338](#)
- [tag-list on page 338](#)
- [target-address on page 339](#)
- [target-parameters on page 340](#)
- [targets on page 341](#)
- [timeout on page 341](#)
- [traceoptions \(SNMP\) on page 342](#)
- [trap-group on page 344](#)
- [trap-options on page 345](#)
- [type \(RMON Notification\) on page 346](#)
- [type \(SNMPv3\) on page 347](#)
- [user on page 347](#)
- [usm on page 348](#)
- [v3 on page 350](#)
- [vacm on page 352](#)
- [variable on page 353](#)
- [version on page 354](#)
- [view \(Configuring a MIB View\) on page 355](#)

- [view \(Associating MIB View with a Community\)](#) on page 356
- [write-view](#) on page 356

access (SNMP)

Syntax	<pre>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) { notify-view <i>view-name</i>; read-view <i>view-name</i>; write-view <i>view-name</i>; } } } } }</pre>
Hierarchy Level	[edit snmp v3 vacm]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set SNMP access limits. The remaining statements are explained separately.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

address (SNMP)

Syntax	<pre>address <i>address</i>;</pre>
Hierarchy Level	[edit snmp v3 target-address <i>target-address-name</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the SNMP target address for receiving traps or informs.
Options	address —IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding the Implementation of SNMP on the QFabric System on page 42• Configuring SNMP on page 121• Example: Configuring SNMP on page 139

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. Statement introduced in Junos OS Release 11.1 on the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define and verify the source addresses for a group of target addresses for SNMP traps and informs.
Options	<i>address-mask</i> —Define a range of addresses.
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"> • <i>Configuring the Address Mask</i>

agent-address

Syntax	<code>agent-address outgoing-interface;</code>
Hierarchy Level	<code>[edit snmp trap-options]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the 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	<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"> • <i>Configuring the Agent Address for SNMP Traps</i>

alarm (SNMP RMON)

Syntax alarm *index* {
 description *description*;
 falling-event-index *index*;
 falling-threshold *integer*;
 falling-threshold-interval *seconds*;
 interval *seconds*;
 request-type (get-next-request | get-request | walk-request);
 rising-event-index *index*;
 rising-threshold *integer*;
 sample-type (absolute-value | delta-value);
 startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
 syslog-subtag *syslog-subtag*;
 variable *oid-variable*;
 }

Hierarchy Level [edit snmp rmon]

Release Information Statement introduced before Junos OS Release 7.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement introduced in Junos OS Release 11.1 for the QFX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure RMON alarm entries.

Options *index*—Identifies this alarm entry as an integer.

 The remaining statements are explained separately.

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

Related Documentation

- [Configuring an RMON Alarm Entry and Its Attributes](#)
- [event \(SNMP\)](#)
- [Configuring RMON Alarms and Events on page 130](#)
- [RMON MIB Event, Alarm, Log, and History Control Tables on page 53](#)
- [Monitoring RMON MIB Tables on page 179](#)
- [Understanding RMON on page 51](#)

authentication-md5

Syntax	authentication-md5 { authentication-password authentication-password; }
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure MD5 as the authentication type for the SNMPv3 user.



NOTE: You can only configure one authentication type for each SNMPv3 user.

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 MD5 Authentication

authentication-none

Syntax	authentication-none;
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure that there should be no authentication for the SNMPv3 user.



NOTE: You can configure only one authentication type for each SNMPv3 user.

Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring No Authentication</i>

authentication-password

Syntax	<code>authentication-password <i>authentication-password</i>;</code>
Hierarchy Level	<code>[edit snmp v3 usm local-engine user <i>username</i> authentication-md5],</code> <code>[edit snmp v3 usm local-engine user <i>username</i> authentication-sha],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> authentication-md5],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> authentication-sha]</code>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the password for user authentication.
Options	<p><i>authentication-password</i>—Password that a user enters. The password is then converted into a key that is used for authentication.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> • The password must be at least eight characters long. • The password can include lowercase letters, uppercase letters, numbers, and the following special characters: <code>.,/\<>;:'[]{}~!@#\$%^*_+=-`</code> <p>In addition, the following special characters are also supported, but you must enclose them within quotation marks ("") if you enter them on the CLI; if you use a Network Management System to enter the password, the quotation marks are not required:</p> <p><code> & () ?</code></p> <p>Control characters—entered by simultaneously pressing the Ctrl key and additional keys—are not supported.</p>
Required Privilege Level	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring MD5 Authentication</i> • <i>Configuring SHA Authentication</i>

authentication-sha

Syntax	<code>authentication-sha { authentication-password authentication-password; }</code>
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the secure hash algorithm (SHA) as the authentication type for the SNMPv3 user.




NOTE: You can configure only one authentication type for each SNMPv3 user.

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">• <i>Configuring SHA Authentication</i>

authorization

Syntax	<code>authorization <i>authorization</i>;</code>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the access authorization for SNMP Get , GetBulk , GetNext , and Set requests.
Options	<p><i>authorization</i>—Access authorization level:</p> <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.
	<div>  <p>NOTE: The read-write option is not supported on the QFX3000 QFabric system.</p> </div>
	Default: read-only
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring the SNMP Community String on page 125

bucket-size

Syntax	<code>bucket-size <i>number</i>;</code>
Hierarchy Level	<code>[edit snmp rmon history <i>index</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the 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	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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• 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 in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define 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 , or startup .
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 on page 126

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 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 on page 127

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 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 on page 127


clients

Syntax	<pre>clients { <i>address</i> <restrict>; }</pre>
Hierarchy Level	<code>[edit snmp community <i>community-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the 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 switch.
Options	<i>address</i> —Address of an SNMP client that is authorized to access this switch. 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 switch.
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 Communities

commit-delay

Syntax	commit-delay <i>seconds</i> ;
Hierarchy Level	[edit snmp nonvolatile]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the timer for the SNMP Set reply and start of the commit.
Options	seconds —Delay between an affirmative SNMP Set reply and start of the commit operation. 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">• <i>Configuring the Commit Delay Timer</i>


community (SNMP)

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 in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define 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.
<hr/>	
<div> NOTE: The authorization read-write option is not supported on the QFX3000 QFabric system.</div> <hr/>	
The SNMP client application specifies an SNMP community name in Get , GetBulk , GetNext , and Set SNMP requests.	
Default	If you omit the community statement, all SNMP requests are denied.
Options	<i>community-name</i> —Community string. If the name includes spaces, enclose it in quotation marks (" "). The remaining statements are explained separately.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the SNMP Community String on page 125

community (RMON)

Syntax	<code>community <i>community-name</i>;</code>
Hierarchy Level	[edit snmp rmon event <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Configure the SNMP trap group that is used when generating a trap (if the eventType object is configured to send traps). If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of eventCommunity). If nothing is configured, traps are sent to each group that has the rmon-alarm category configured.</p> <p>The event community is not the same as an SNMP community.</p>
Options	<i>community-name</i> —Name of the trap group that is used when generating a trap if the event is configured to send traps.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

community-name (SNMP)

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. Statement introduced in Junos OS Release 11. for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define an SNMP community to authorize SNMPv1 or SNMPv2c clients in an SNMPv3 system. When you configure a community in SNMPv3, you can also specify a security name. The access privileges associated with the security name determine which MIB objects are available and which operations (read, write, or notify) are 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 the name 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> <p>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).</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"><i>Configuring the SNMPv3 Community</i>

contact

Syntax	<code>contact <i>contact</i>;</code>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define 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">• <i>Configuring the System Contact on a Device Running Junos OS</i>

description (SNMP)

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define the value of the MIB II sysDescription object, which is the description of the system being managed.
Default	By default, the sysDescription object includes the following information: Juniper Networks, Inc. <i>platform</i> , <i>build</i> , Build date: <i>date</i> UTC Copyright (c) <i>date-range</i> Juniper Networks, Inc. For example: sysDescr.0 = Juniper Networks, Inc. m7i internet router, kernel JUNOS 13.2-20130530_ib_13_3_psd.1, Build date: 2013-05-30 22:48:07 UTC Copyright (c) 1996-2013 Juniper Networks, Inc.
Options	<i>description</i> —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">• <i>Configuring the System Description on a Device Running Junos OS</i>


description (RMON)

Syntax	<code>description</code> <i>description</i> ;
Hierarchy Level	[edit snmp rmon alarm <i>index</i>], [edit snmp rmon event <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Text description of alarm or event.
Options	<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"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

destination-port (SNMP)

Syntax	<code>destination-port</code> <i>port-number</i> ;
Hierarchy Level	[edit snmp trap-group]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	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 on page 126

engine-id

Syntax	<pre>engine-id { (local <i>engine-id-suffix</i> use-default-ip-address use-mac-address); }</pre>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Define a unique identifier for an SNMPv3 engine by configuring the suffix of the engine ID. The engine ID is used for identification only and not for addressing. There are two parts of an engine ID: the prefix and the suffix. The prefix is formatted according to the specifications defined in RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> and cannot be configured. The suffix is configured here.</p> <div><p>NOTE: SNMPv3 authentication and encryption keys are generated based on the associated user passwords and the engine ID. If you configure or change the engine ID, you must commit the user passwords and new engine ID before you configure SNMPv3 users, or the authentication will fail.</p><p>By default, the engine ID suffix is configured with the MAC address of the management interface (the <i>use-mac-address</i> option) on the QFX Series and OCX Series. You can override this configuration by using the <i>local engine-id-suffix</i> or <i>use-default-ip-address</i> option.</p></div>
Default	<i>use-mac-address</i>
Options	<p><i>local engine-id-suffix</i>—The engine ID suffix is set based on the data entered.</p> <p><i>use-default-ip-address</i>—The engine ID suffix is generated from the default IP address.</p> <p><i>use-mac-address</i>—The engine ID suffix is generated from the MAC address of the management interface on the switch.</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">• SNMPv3 Overview on page 49• Configuring SNMP on page 121• Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50

event

Syntax	<pre>event <i>index</i> { <i>community</i> <i>community-name</i>; <i>description</i> <i>description</i>; type (RMON Notification) <i>type</i>; }</pre>
Hierarchy Level	[edit snmp rmon]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure RMON event entries.
Options	<i>index</i> —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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

falling-event-index (RMON)

Syntax	<code>falling-event-index <i>index</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the index number of the event entry that is used when a falling threshold is crossed. You specify the falling-event index when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.
Options	<i>index</i> —Index of the event entry that is used when a falling threshold is crossed. Range: 0 through 65,535 Default: 0
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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

falling-threshold (Health Monitor)

Syntax	<code>falling-threshold <i>percentage</i>;</code>
Hierarchy Level	[edit snmp health-monitor]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.
Options	<i>percentage</i> —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">• rising-threshold on page 316• Configuring Health Monitoring on page 132

falling-threshold (RMON)

Syntax	<code>falling-threshold <i>integer</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the lower threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.
Options	<i>integer</i> —Lower threshold for the alarm entry. Range: -2,147,483,648 through 2,147,483,647 Default: 20 percent less than the rising-threshold value
Required Privilege Level	snmp —To view this statement in the configuration. snmp-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

falling-threshold-interval

Syntax	<code>falling-threshold-interval <i>seconds</i>;</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the interval between samples after the rising threshold is exceeded and the value of the sample starts to drop. If the value of the sample drops and exceeds the falling threshold, the regular sampling interval is used.
Options	<i>interval</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"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

filter-duplicates

Syntax	<code>filter-duplicates;</code>
Hierarchy Level	<code>[edit snmp]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	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"> • Understanding the Implementation of SNMP on the QFabric System on page 42 • Example: Configuring SNMP on page 139

filter-interfaces

Syntax	<pre>filter-interfaces { all-internal-interfaces; interfaces <i>interface</i> }</pre>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	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—Filter out information from SNMP Get and GetNext requests for all internal interfaces.</p> <p>interfaces—Filter out information from SNMP Get and GetNext requests for the specified interface.</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">• <i>Filtering Interface Information Out of SNMP Get and GetNext Output</i>

group (Associating a Security Name)

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. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate a security name with a group composed of users with the same access privileges. The security name is used during authentication of SNMP messages, and is mapped to a username.
Options	<i>group-name</i> —Collection of SNMP security names that share the same SNMPv3 access privileges.
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"> • <i>Configuring the Group</i>

group (Configuring Access Privileges)

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.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The **default-context-prefix** statement, when included, adds all the contexts configured on the device to the group, whereas the **context-prefix context-prefix** statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series and OCX Series.) When the context prefix is specified as default (for example, **context-prefix default**), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as **logical system/routing instance**. For example, to specify routing instance ri1 in logical system ls1, include **context-prefix ls1/ri1**.

The remaining statements under this hierarchy are explained separately.

Options *group-name*—SNMPv3 group name created for the SNMPv3 group.

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

Related Documentation • *Configuring the Group*

health-monitor

Syntax	<pre>health-monitor { falling-threshold <i>percentage</i>; interval <i>seconds</i>; rising-threshold <i>percentage</i>; }</pre>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure 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 page 132• Understanding Health Monitoring on page 55

history

Syntax	<pre>history <i>history-index</i> { <i>bucket-size</i> <i>number</i>; <i>interface</i> <i>interface-name</i>; <i>interval</i> <i>seconds</i>; <i>owner</i> <i>owner-name</i>; }</pre>
Hierarchy Level	[edit snmp rmon]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Configure RMON history group entries. This RMON feature can be used with the Simple Network Management Protocol (SNMP) agent on the network to monitor all the traffic flowing among devices on all connected LAN segments. The RMON history feature 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. If you use the history statement, you must also configure the interface <i>interface-name</i> statement.</p>
Options	<p>history-index—Provide a number for this history entry.</p> <p>Range: 1 through 65535</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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

interface (SNMP)

Syntax	<code>interface [<i>interface-names</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. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the interfaces on which SNMP requests can be accepted.
Default	If you omit this statement, SNMP requests entering the router or switch through any interface are accepted.
Options	<i>interface-names</i> —Names of one or more logical interfaces.
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 Interfaces on Which SNMP Requests Can Be Accepted on page 128

interface (RMON)

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 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Specify the interface to be monitored in the specified RMON history entry.</p> <p>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.</p>
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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

interval (Health Monitor)

Syntax	interval <i>seconds</i> ;
Hierarchy Level	[edit snmp health-monitor]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the interval between sampling of the object being monitored by the health monitor.
Options	seconds —Time between samples, in seconds. Range: 1 through 2147483647 seconds Default: 300 seconds
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Health Monitoring on page 132

interval (RMON)

Syntax	<code>interval <i>seconds</i>;</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>], [edit snmp rmon history <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the interval over which data is to be sampled for the specified alarm or interface.
Default	60 sec for alarm sampling. 1800 sec for history sampling.
Options	<i>seconds</i> —Interval at which data is to be sampled for the specified alarm or 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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

local-engine

Syntax

```
local-engine {
  user username {
    authentication-md5 {
      authentication-password authentication-password;
    }
    authentication-none;
    authentication-sha {
      authentication-password authentication-password;
    }
    privacy-aes128 {
      privacy-password privacy-password;
    }
    privacy-des {
      privacy-password privacy-password;
    }
    privacy-3des {
      privacy-password privacy-password;
    }
    privacy-none {
      privacy-password privacy-password;
    }
  }
}
```

Hierarchy Level [edit snmp v3 [usm](#)]

Release Information Statement introduced before Junos OS Release 7.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement introduced in Junos OS Release 11.1 for the QFX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure local engine information for the user-based security model (USM).
 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

- [Creating SNMPv3 Users on page 133](#)

location

Syntax	<code>location <i>location</i>;</code>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Define the value of the MIB II sysLocation object, which is the physical location of the managed system.
Options	<i>location</i> —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">• <i>Configuring the System Location for a Device Running Junos OS</i>

logical-system (SNMP)

Syntax	<pre>logical-system <i>logical-system-name</i> { <i>routing-instance routing-instance-name</i>; }</pre>
Hierarchy Level	<pre>[edit snmp community <i>community-name</i>], [edit snmp trap-group], [edit snmp trap-options] [edit snmp v3target-address <i>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> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<div style="display: flex; align-items: center;">  <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> </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"> <i>Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community</i> <i>Configuring the Trap Target Address</i>

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the message processing model to be used when generating SNMP notifications.
Options	v1 —SNMPv1 message process model. v2c —SNMPv2c message process model. v3 —SNMPv3 message process model.
Required Privilege Level	snmp —To view this statement in the configuration. snmp-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Message Processing Model</i>

name

Syntax	<code>name <i>name</i>;</code>
Hierarchy Level	<code>[edit snmp]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the system name from the command-line interface.
Options	<i>name</i> —System name override.
Required Privilege Level	snmp —To view this statement in the configuration. snmp-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the System Name</i>

nonvolatile

Syntax	<code>nonvolatile { commit-delay seconds; }</code>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure 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">• <i>Configuring the Commit Delay Timer</i>• <i>commit-delay</i>

notify

Syntax	<pre>notify <i>name</i> { tag <i>tag-name</i>; type (trap inform); }</pre>
Hierarchy Level	[edit snmp v3]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>type inform option added in 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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<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">• <i>Configuring the Inform Notification Type and Target Address</i>• <i>Configuring the SNMPv3 Trap Notification</i>

notify-filter (Applying to the Management Target)

Syntax	<code>notify-filter <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-parameters <i>target-parameters-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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the notify filter applied to a specific set of SNMPv3 target parameters. Target parameters are the message processing and security parameters for notifications sent to a target SNMP manager.
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"> • <i>Applying the Trap Notification Filter</i>

notify-filter (Configuring the Profile Name)

Syntax	<code>notify-filter <i>profile-name</i> { oid <i>oid</i> (include exclude); }</code>
Hierarchy Level	<code>[edit snmp v3]</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify a group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.
Options	<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"> • <i>Configuring the Trap Notification Filter</i> • <i>oid (SNMP)</i>

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).
Options	<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 Views on page 129• Configuring 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 in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify an object identifier (OID) used to represent a subtree of MIB objects.
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 on page 129

oid (SNMPv3)

Syntax	oid <i>oid</i> (include exclude);
Hierarchy Level	[edit snmp v3 notify-filter <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify 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"> • SNMPv3 Overview on page 49 • Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50 • Configuring SNMP on page 121 • Configuring the SNMPv3 Trap Notification

owner

Syntax	<code>owner owner-name;</code>
Hierarchy Level	[edit snmp rmon history <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the user or group responsible for this RMON history configuration.
Options	owner-name —User or group responsible for this configuration. Range: 0 through 32 alphanumeric characters
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• 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	<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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure a set of target parameters for message processing and 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"> • <i>Defining and Configuring the Trap Target Parameters</i>

port (SNMP)

Syntax	port <i>port-number</i> ;
Hierarchy Level	[edit snmp v3 target-address <i>target-address-name</i>]
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<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"> • <i>Configuring the Port</i>

privacy-3des

Syntax	<pre>privacy-3des { privacy-password <i>privacy-password</i>; }</pre>
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.
Options	<p>privacy-password <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none">• The password must be at least eight characters long.• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the SNMPv3 Encryption Type</i>

privacy-aes128

Syntax	<pre>privacy-aes128 { privacy-password <i>privacy-password</i>; }</pre>
Hierarchy Level	<pre>[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i>]</pre>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.</p>
Options	<p>privacy-password <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> • The password must be at least eight characters long. • The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
Required Privilege Level	<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"> • <i>Configuring the SNMPv3 Encryption Type</i>

privacy-des

Syntax	<pre>privacy-des { privacy-password <i>privacy-password</i>; }</pre>
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.
Options	<p>privacy-password <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none">• The password must be at least eight characters long.• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the SNMPv3 Encryption Type</i>

privacy-none

Syntax	privacy-none;
Hierarchy Level	[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure that no encryption be used for the SNMPv3 user.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the SNMPv3 Encryption Type</i>

privacy-password

Syntax	<code>privacy-password <i>privacy-password</i>;</code>
Hierarchy Level	<code>[edit snmp v3 usm local-engine user <i>username</i> privacy-3des],</code> <code>[edit snmp v3 usm local-engine user <i>username</i> privacy-aes128],</code> <code>[edit snmp v3 usm local-engine user <i>username</i> privacy-des],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-3des],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-aes128],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-des]</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure a privacy password for the SNMPv3 user.
Options	<p><i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none">• The password must be at least eight characters long.• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
Required Privilege Level	<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">• <i>Configuring the SNMPv3 Encryption Type</i>

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • <i>Configuring the Read View</i> • Configuring MIB Views on page 129

remote-engine

Syntax	<pre> remote-engine <i>engine-id</i> { user <i>username</i> { authentication-md5 { authentication-password <i>authentication-password</i>; } authentication-none; authentication-sha { authentication-password <i>authentication-password</i>; } privacy-aes128 { privacy-password <i>privacy-password</i>; } privacy-des { privacy-password <i>privacy-password</i>; } privacy-3des { privacy-password <i>privacy-password</i>; } privacy-none { privacy-password <i>privacy-password</i>; } } } </pre>
Hierarchy Level	[edit snmp v3 usm]
Release Information	<p>Statement introduced in 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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.
Options	<p><i>engine-id</i>—Specify engine identifier in hexadecimal format. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.</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"> <i>Configuring the Remote Engine and Remote User</i>

request-type

Syntax	<code>request-type (get-next-request get-request walk-request);</code>
Hierarchy Level	<code>[edit snmp rmon alarm <i>index</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Extend monitoring to a specific SNMP object instance (<code>get-request</code>), to all object instances belonging to a MIB branch (<code>walk-request</code>), or to the next object instance after the instance specified in the configuration (<code>get-next-request</code>).
Default	<code>walk-request</code>
Options	<p><code>get-next-request</code>—Perform an SNMP get next request.</p> <p><code>get-request</code>—Perform an SNMP get request.</p> <p><code>walk-request</code>—Perform an SNMP walk request.</p>
Required Privilege Level	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

retry-count (SNMPv3)

Syntax	<code>retry-count <i>number</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the retry count for SNMP informs.
Options	<i>number</i> —Maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded. Default: 3 times
Required Privilege Level	<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 Informs on page 138• <code>timeout</code>

rising-event-index

Syntax	<code>rising-event-index <i>index</i>;</code>
Hierarchy Level	[edit snmp rmon alarm index]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the index of the event entry that is used when a rising alarm threshold is exceeded. The rising-event index is specified when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.
Options	<i>index</i> —Index of the event entry that is used when a rising threshold is exceeded. Range: 0 through 65,535 Default: 0
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"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

rising-threshold (Health Monitor)

Syntax	<code>rising-threshold <i>percentage</i>;</code>
Hierarchy Level	[edit snmp health-monitor]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.
Options	<i>percentage</i> —Upper threshold for the alarm entry. Range: 1 through 100 Default: 80 percent of the maximum possible value
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Health Monitoring on page 132• falling-threshold on page 283

rising-threshold (RMON)

Syntax	rising-threshold <i>integer</i> ;
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the upper threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.
Options	<i>integer</i> —Upper threshold for the alarm entry. Range: -2,147,483,648 through 2,147,483,647
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

rmon

```
Syntax  rmon {
        alarm index {
            description description;
            falling-event-index index;
            falling-threshold integer;
            falling-threshold-interval seconds;
            interval seconds;
            request-type;
            rising-event-index index;
            rising-threshold integer;
            sample-type (absolute-value | delta-value);
            startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
            syslog-subtag syslog-subtag;
            variable oid-variable;
        }
        event index {
            community community-name;
            description description;
            type (RMON Notification) type;
        }
        history history-index {
            bucket-size number;
            interface interface-name;
            interval seconds;
            owner owner-name;
        }
    }
```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Provide comprehensive network fault diagnosis, planning, and performance tuning information. RMON delivers this information in nine groups of monitoring elements, each providing specific sets of data to meet common network monitoring requirements. Each group is optional, so that vendors do not need to support all the groups within the MIB.

Junos OS supports the RMON statistics, history, alarm, and event groups.

The remaining statements are explained separately.

Default Disabled.


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

Related Documentation

- [RMON MIB Event, Alarm, Log, and History Control Tables on page 53](#)
- [Monitoring RMON MIB Tables on page 179](#)

- [Understanding RMON on page 51](#)
- [Junos OS Network Management Configuration Guide](#)

routing-instance (SNMP)

Syntax	<code>routing-instance <i>routing-instance-name</i> { source-address <i>source-address</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.
<div>  NOTE: In releases 14.1R3 and later, Junos OS supports IPv6 source addresses of the SNMP traps. </div>	
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

sample-type

Syntax	sample-type (absolute-value delta-value);
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the method of sampling the selected variable (monitored object). When you configure an SNMP RMON alarm, you can specify the sample type.
Options	<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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

security-level (Defining Access Privileges)

Syntax	<pre>security-level (authentication none privacy) { notify-view view-name; read-view view-name; write-view view-name; }</pre>
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)]
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Define the security level used for access privileges.
Default	none
Options	<p>authentication—Provide authentication but no encryption.</p> <p>none—No authentication and no encryption.</p> <p>privacy—Provide authentication and encryption.</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"> • <i>Configuring the Security Level</i>

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• <i>Configuring the Security Level</i>

security-model (Access Privileges)

Syntax	<code>security-model (usm v1 v2c);</code>
Hierarchy Level	<code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix context-prefix <i>context-prefix</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • <i>Configuring the Security Model</i>


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	<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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Define a security model for an SNMPv3 group and associate the security name of a user with the group. All users in the group have the same access privileges.
Options	<p>usm—SNMPv3 security model.</p> <p>v1—SNMPv1 security model.</p> <p>v2c—SNMPv2c security model.</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">• <i>Configuring the Security Model</i>

security-model (SNMP Notifications)

Syntax	<code>security-model (usm v1 v2c);</code>
Hierarchy Level	<code>[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]</code>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the security model for an SNMPv3 group. The security model is used for SNMP notifications.
Options	<p>usm—SNMPv3 security model.</p> <p>v1—SNMPv1 security model.</p> <p>v2c—SNMPv2c security model.</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"> • <i>Configuring the Security Model</i>


security-name (Community String)

Syntax	<code>security-name <i>security-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. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level.
Options	<i>security-name</i> —Name that is used for messaging security and user access control.
<div> NOTE: The security name must match the configured security name at the <code>[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]</code> hierarchy level when you configure traps or informs.</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"><i>Configuring the Security Names</i>

security-name (Security Group)

Syntax	<code>security-name <i>security-name</i> { group <i>group-name</i>; }</code>
Hierarchy Level	[edit snmp v3 vacm security-to-group security-model (usm v1 v2c)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate the security name of a user (for SNMPv3 clients) or a community string (for SNMPv1 and SNMPv2c clients) with a configured security group.
Options	security-name —SNMPv3 secure username configured at the [edit snmp v3 usm local-engine user <i>username</i>] hierarchy level that is used for messaging security. For SNMPv1 and SNMPv2c, the security name is the community string configured at the [edit snmp v3 snmp-community community-index] hierarchy level.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Assigning Security Names to Groups</i> • Assigning a Security Name to a Group on page 136

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• <i>Configuring the Security Name</i>

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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • <i>Assigning Security Model and Security Name to a Group</i>

snmp

```
Syntax snmp {
    client-list client-list-name {
        ip-addresses;
    }
    community community-name {
        authorization authorization;
        client-list-name client-list-name;
        clients {
            address restrict;
        }
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                clients {
                    addresses;
                }
            }
        }
        routing-instance routing-instance-name {
            clients {
                addresses;
            }
        }
        view view-name;
    }
    contact contact;
    description description;
    filter-duplicates;
    filter-interfaces;
    health-monitor {
        falling-threshold integer;
        interval seconds;
        rising-threshold integer;
    }
    interface [ interface-names ];
    location location;
    name name;
    nonvolatile {
        commit-delay seconds;
    }
    rmon {
        alarm index {
            description description;
            falling-event-index index;
            falling-threshold integer;
            falling-threshold-interval seconds;
            interval seconds;
            request-type;
            rising-event-index index;
            rising-threshold integer;
            sample-type (absolute-value | delta-value);
            startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
            syslog-subtag syslog-subtag;
        }
    }
}
```



```

    variable oid-variable;
}
event index {
    community community-name;
    description description;
    type type;
}
history history-index {
    bucket-size number;
    interface interface-name;
    interval seconds;
    owner owner-name;
}
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regular-expression>;
    flag flag;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance routing-instance-name;
        tag-list tag-list;
        target-parameters target-parameters-name;
    }
}

```



```
    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | V3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
  usm {
    local-engine {
      user username {
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none;
      }
    }
    remote-engine engine-id {
      user username {
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none {
          privacy-password privacy-password;
        }
      }
    }
  }
}
```



```

}
vacm {
  access {
    group group-name {
      (default-context-prefix | context-prefix context-prefix) {
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}
view view-name {
  oid object-identifier (include | exclude);
}
}
}

```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure SNMP.

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

- [Understanding the Implementation of SNMP on page 39](#)
- [Configuring SNMP on page 121](#)

snmp-community

Syntax	<pre>snmp-community <i>community-index</i> { <i>community-name</i> <i>community-name</i>; <i>security-name</i> <i>security-name</i>; tag <i>tag-name</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. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the SNMP community which authorizes SNMPv1 or SNMPv2c clients in an SNMPv3 system.
Options	<i>community-index</i> —(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">• <i>Configuring the SNMPv3 Community</i>

source-address (SNMP)

Syntax	source-address <i>address</i> ;
Hierarchy Level	[edit snmp trap-options]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the source address of every SNMP trap packet sent by this switch 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 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">• <i>Configuring the Source Address for SNMP Traps</i>

startup-alarm

Syntax	startup-alarm (falling-alarm rising-alarm rising-or-falling-alarm);
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set an initial alarm that is sent after the configured SNMP RMON alarm becomes active.
Default	rising-or-falling-alarm
Options	<p>falling-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the falling threshold.</p> <p>rising-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the rising threshold.</p> <p>rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active is equal to or greater than either the rising threshold or the falling threshold.</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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

syslog-subtag

Syntax	<code>syslog-subtag <i>syslog-subtag</i>;</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Add the syslog-subtag tag to the system log message. The tag should not exceed 80 uppercase characters.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

tag (Configuring Notification Targets)

Syntax	<code>tag <i>tag-name</i>;</code>
Hierarchy Level	[edit snmp v3 notify <i>name</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure a set of target addresses to receive SNMP traps or informs (for IPv4 packets only).
Options	tag-name —Define the target addresses to which an SNMP notification is sent. Target addresses containing the same tag in their tag list are sent the same notification. The tag-name is not included in the notification.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • SNMPv3 Overview on page 49 • Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50 • Configuring SNMP on page 121 • Configuring the SNMPv3 Trap Notification

tag (Configuring the SNMP Community)

Syntax	<code>tag tag-name;</code>
Hierarchy Level	<code>[edit snmp v3 snmp-community community-index]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure a set of SNMP managers that are authorized to use a community string.
Options	tag-name —Identify the set of addresses for the SNMP managers authorized to use the 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">• SNMPv3 Overview on page 49• Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50• Configuring SNMP on page 121• Configuring the SNMPv3 Trap Notification

tag-list

Syntax	<code>tag-list tag-list;</code>
Hierarchy Level	<code>[edit snmp v3 target-address target-address-name]</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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>; port <i>port-number</i>; retry-count <i>number</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	<p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<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"> • Understanding the Implementation of SNMP on page 39 • SNMP MIBs Support on page 56 • SNMP Traps Support on page 72 • snmp on page 330 • Configuring SNMP on page 121 • Monitoring SNMP on page 179 • Example: Configuring SNMP on page 139

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.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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 snmp—To view this statement in the configuration.
Level 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 { <i>address</i>; }</code>
Hierarchy Level	<code>[edit snmp trap-group <i>group-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure 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 on page 126

timeout

Syntax	<code>timeout <i>seconds</i>;</code>
Hierarchy Level	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the timeout period (in seconds) for SNMP informs.
Default	15 seconds
Options	<i>seconds</i> —Number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted.
Required Privilege Level	<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"> • Understanding the Implementation of SNMP on page 39 • Configuring SNMP Informs on page 138 • retry-count (SNMPv3) on page 314

traceoptions (SNMP)

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	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Track the activities of SNMP agents on the switch and record the information in log files.



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

The output of the tracing operations is placed into log files in the **/var/log** directory. Each log file is named after the SNMP agent that generates it. The following logs are created in the **/var/log** directory when the **traceoptions** statement is used:

- chassisd
- craftd
- ilmid
- mib2d
- rmopd
- serviced
- snmpd

Options **file *filename***—By default, the name of the log file that records trace output is the name of the process being traced (for example, mib2d or snmpd). Use this option to specify another name.

files *number*—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, snmpd) reaches its maximum size, it is archived by being renamed to snmpd.0. The previous snmpd.1 is renamed to snmpd.2, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements:

- **all**—Log all SNMP events.

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

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

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

Range: 10 KB through 1 GB

Default: 1000 KB

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

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

Related Documentation

- [Understanding Tracing and Logging Operations on page 7](#)
- [Tracing SNMP Activity on a Device Running Junos OS on page 183](#)

trap-group

Syntax	<pre>trap-group <i>group-name</i> { categories { category; } destination-port <i>port-number</i>; targets { address; } }</pre>
Hierarchy Level	[edit snmp]
Release Information	Statement introduced in Junos OS Release 11.1 for QFX Series switches. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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	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 on page 126

trap-options

Syntax	<pre>trap-options { agent-address outgoing-interface; source-address address; }</pre>
Hierarchy Level	[edit snmp]
Release Information	<p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<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"> • <i>Configuring SNMP Trap Options</i>

type (RMON Notification)

Syntax	<code>type type;</code>
Hierarchy Level	[edit snmp rmon event <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the type of notification generated when a rising or falling threshold is crossed.
Default	<code>log-and-trap</code>
Options	type —Type of notification. It can be one of the following: <ul style="list-style-type: none">• log—Add an entry to the logTable object.• log-and-trap—Send an SNMP trap and add a log entry.• none—No notifications are sent.• snmptrap—Send an SNMP trap.
Required Privilege Level	<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">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Configuring RMON Alarms and Events on page 130• Monitoring RMON MIB Tables on page 179• Understanding RMON on page 51• Junos OS Network Management Configuration Guide

type (SNMPv3)

Syntax	<code>type (inform trap);</code>
Hierarchy Level	<code>[edit snmp v3 notify <i>name</i>]</code>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>inform option added in 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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring SNMP Informs on page 138 • Configuring the SNMPv3 Trap Notification

user

Syntax	<code>user <i>username</i>;</code>
Hierarchy Level	<p><code>[edit snmp v3 usm local-engine],</code></p> <p><code>[edit snmp v3 usm remote-engine <i>engine-id</i>]</code></p>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Specify a user associated with an SNMPv3 group on a local or remote SNMP engine.
Options	username —SNMPv3 user-based security model (USM) username.
Required Privilege Level	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating SNMPv3 Users on page 133

usm

```

Syntax  usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-none;
                authentication-sha {
                    authentication-password authentication-password;
                }
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-3des {
                    privacy-password privacy-password;
                }
                privacy-none {
                    privacy-password privacy-password;
                }
            }
        }
        remote-engine engine-id {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-none;
                authentication-sha {
                    authentication-password authentication-password;
                }
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-3des {
                    privacy-password privacy-password;
                }
                privacy-none {
                    privacy-password privacy-password;
                }
            }
        }
    }
}

```

Hierarchy Level [edit snmp v3]

Release Information Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure user-based security model (USM) 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

- [Creating SNMPv3 Users on page 133](#)
- *Configuring the Remote Engine and Remote User*

v3

```

Syntax v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        port port-number;
        retry-count number;
        tag-list tag-list;
        target-parameters target-parameters-name;
        timeout seconds;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | v3);
            security-level (authentication | none | privacy);
            security-model (usm | v1 | v2c);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-sha {
                    authentication-password authentication-password;
                }
                authentication-none;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
            privacy-3des {
                privacy-password privacy-password;
            }
            privacy-none;
        }
    }
}

```



```

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

```

Hierarchy Level [edit snmp]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description	Configure SNMPv3. The remaining statements are explained separately.
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 on page 50

vacm

Syntax	<pre> 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; } } } </pre>
Hierarchy Level	[edit snmp v3]
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure view-based access control model (VACM) information, including access privileges such as security model and security level for a group of users.</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"> • <i>Defining Access Privileges for an SNMP Group</i>


variable

Syntax	<code>variable <i>oid-variable</i>;</code>
Hierarchy Level	[edit snmp rmon alarm <i>index</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Set the object identifier (OID) of the MIB object (also called variable) to be monitored when you configure an SNMP RMON alarm. If the value of the monitored variable exceeds the configured rising threshold or falling threshold, an alarm is triggered and a corresponding event may be generated.
Options	<i>oid-variable</i> —OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, 1.3.6.1.2.1.2.1.2.1.10.1) or the name of the MIB object—for example, ifInOctets.1 .
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Configuring RMON Alarms and Events on page 130 • Monitoring RMON MIB Tables on page 179 • Understanding RMON on page 51 • Junos OS Network Management Configuration Guide

version

Syntax	version (all v1 v2);
Hierarchy Level	[edit snmp trap-group <i>group-name</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the version number of SNMP traps.
Default	all—Send an SNMPv1 and SNMPv2 trap for every trap condition.
Options	all—Send an SNMPv1 and SNMPv2 trap for every trap condition. v1—Send SNMPv1 traps only. v2—Send SNMPv2 traps only.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SNMP Trap Groups on page 126

view (Configuring a MIB View)

Syntax	<pre>view <i>view-name</i> { <i>oid object-identifier</i> (include exclude); }</pre>
Hierarchy Level	[edit snmp]
Release Information	<p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>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 <i>community-name</i>] hierarchy level.</p>
	<div>  <p>NOTE: To remove an OID completely, use the delete view all oid oid-number command but omit the include parameter.</p> </div>
Options	<p><i>view-name</i>—Name of the view.</p> <p>The remaining statement is 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 MIB Views on page 129 • Associating MIB Views with an SNMP User Group • community on page 274

view (Associating MIB View with a Community)

Syntax	<code>view view-name;</code>
Hierarchy Level	<code>[edit snmp community community-name]</code>
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate a view with a community. A view represents a group of MIB objects.
Options	view-name —Name of the view. You must use a view name already configured in the view statement at the <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">• <i>Configuring SNMP Communities</i>

write-view

Syntax	<code>write-view view-name;</code>
Hierarchy Level	<code>[edit snmp v3 vacm access group group-name (default-context-prefix context-prefix context-prefix) security-model (any usm v1 v2c) security-level (authentication none privacy)]</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. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).
Options	view-name —Name of the view for which the SNMP user group has write permission.
Required Privilege Level	snmp —To view this statement in the configuration. snmp-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MIB Views on page 129• <i>Configuring the Write View</i>

CHAPTER 22

Configuration Statements for System Log Messages

- [archive \(All System Log Files\) on page 358](#)
- [archive \(Individual System Log File\) on page 360](#)
- [archive \(QFabric System\) on page 361](#)
- [console \(System Logging\) on page 362](#)
- [explicit-priority on page 363](#)
- [facility-override on page 364](#)
- [file \(QFabric System\) on page 365](#)
- [file \(System Logging\) on page 366](#)
- [files on page 367](#)
- [host \(System\) on page 368](#)
- [log-prefix \(System\) on page 370](#)
- [match on page 370](#)
- [size \(System\) on page 371](#)
- [structured-data on page 372](#)
- [syslog \(System\) on page 373](#)
- [syslog \(QFabric System\) on page 375](#)
- [time-format on page 376](#)
- [user \(System Logging\) on page 377](#)

archive (All System Log Files)

Syntax	<code>archive <files <i>number</i>> <size <i>size</i>> <start-time <i>time</i>> <transfer-interval <i>interval</i>> <binary-data no-binary-data>; <world-readable no-world-readable> ;</code>
Hierarchy Level	[edit system syslog]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure archiving properties for all system log files.
Options	<p>files <i>number</i>—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file logfile, it closes the file, compresses it, and renames it logfile.0.gz (the amount of data is determined by the size statement at this hierarchy level). The utility then opens and writes to a new file called logfile. When the new file reaches the maximum size, the logfile.0.gz file is renamed to logfile.1.gz, and the new file is closed, compressed, and renamed logfile.0.gz. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).</p> <p>Range: 1 through 1000</p> <p>Default: 10 files</p> <p>size <i>size</i>—Maximum amount of data that the Junos OS logging utility writes to a log file logfile before archiving it (closing it, compressing it, and changing its name to logfile.0.gz). The utility then opens and writes to a new file called logfile.</p> <p>Syntax: <i>x k</i> to specify the number of kilobytes, <i>x m</i> for the number of megabytes, or <i>x g</i> for the number of gigabytes</p> <p>Range: 64 KB through 1 GB</p> <p>Default:</p> <ul style="list-style-type: none">• 128 KB for EX Series switches and J Series routers• 1 MB for M Series, MX Series, and T Series routers, OCX Series, and the QFX3500 switch• 10 MB for TX Matrix and TX Matrix Plus routers <p>binary-data no-binary-data—Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems)..</p> <p>Default: no-binary-data</p> <p>world-readable no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the root user and users who have the Junos OS maintenance permission.</p>

Default: no-world-readable

Required Privilege Level	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying Log File Size, Number, and Archiving Properties on page 157

archive (Individual System Log File)

Syntax	<code>archive <archive-sites (<i>ftp-url</i> <password <i>password</i>>)> <files <i>number</i>> <size <i>size</i>> <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval <i>minutes</i>> <world-readable no-world-readable>;</code>
Hierarchy Level	[edit system syslog file <i>filename</i>]
Release Information	Statement introduced before Junos OS Release 7.4. start-time and transfer-interval statements introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure archiving properties for a specific system log file.
Options	<p>archive-sites <i>site-name</i>—FTP URL representing the destination for the archived log file (for information about how to specify valid FTP URLs, see <i>Format for Specifying Filenames and URLs in Junos OS CLI Commands</i>). If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the filename specified at the [edit system syslog] hierarchy level.</p> <p>files <i>number</i>—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <i>logfile</i>, it closes the file, compresses it, and renames it <i>logfile.0.gz</i> (the amount of data is determined by the size statement at this hierarchy level). The utility then opens and writes to a new file called <i>logfile</i>. When the new file reaches the maximum size, the <i>logfile.0.gz</i> file is renamed to <i>logfile.1.gz</i>, and the new file is closed, compressed, and renamed <i>logfile.0.gz</i>. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).</p> <p>Range: 1 through 1000</p> <p>Default: 10 files</p> <p>password <i>password</i>—Password for authenticating with the site specified by the archive-sites statement.</p> <p>size <i>size</i>—Maximum amount of data that the Junos OS logging utility writes to a log file <i>logfile</i> before archiving it (closing it, compressing it, and changing its name to <i>logfile.0.gz</i>). The utility then opens and writes to a new file called <i>logfile</i>.</p> <p>Syntax: <i>xk</i> to specify the number of kilobytes, <i>xm</i> for the number of megabytes, or <i>xg</i> for the number of gigabytes</p> <p>Range: 64 KB through 1 GB</p> <p>Default: 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, OCX Series, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers</p>

start-time "YYYY-MM-DD.hh:mm"—Date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval *interval*—Interval at which to transfer the log file to an archive site.

Range: 5 through 2880 minutes

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

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

Related Documentation • [Specifying Log File Size, Number, and Archiving Properties on page 157](#)

archive (QFabric System)

Syntax archive {
size *size*;
}

Hierarchy Level [edit system [syslog](#) file *filename*]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Configure the archiving properties for the system message log file.

Options **size *size***—Maximum amount of system log message data that the QFabric system stores in the log file.

Syntax: *xk* to specify the number of kilobytes, *xm* for the number of megabytes, or *xg* for the number of gigabytes

Range: 65 KB through 1 GB

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

Related Documentation • [syslog on page 375](#)

console (System Logging)

Syntax	<code>console { <i>facility severity</i>; }</code>
Hierarchy Level	[edit system syslog]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the logging of system messages to the system console.
Options	<i>facility</i> —Class of messages to log. To specify multiple classes, include multiple <i>facility severity</i> statements. For a list of the facilities, see Table 27 on page 159 . <i>severity</i> —Severity of the messages that belong to the facility specified by the paired <i>facility</i> name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 28 on page 160 .
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">• Directing System Log Messages to the Console on page 148• <i>Junos OS System Log Messages Reference</i>

explicit-priority

Syntax	explicit-priority;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i>], [edit logical-systems <i>logical-system-name</i> system syslog host], [edit system syslog file <i>filename</i>], [edit system syslog host]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination. When the structured-data statement is also included at the [edit system syslog file <i>filename</i>] hierarchy level, this statement is ignored for the file.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Including Priority Information in System Log Messages on page 150 • <i>Junos OS System Log Messages Reference</i> • structured-data on page 372

facility-override

Syntax	<code>facility-override <i>facility</i>;</code>
Hierarchy Level	[edit system syslog host]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.
Options	<i>facility</i> —Alternate facility to substitute for the default facilities. For a list of the possible facilities, see Table 30 on page 161 .
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">• Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination on page 162• <i>Junos OS System Log Messages Reference</i>

file (QFabric System)

Syntax	<pre>file <i>filename</i> { archive { <i>size</i> <i>maximum-file-size</i>; } <i>explicit-priority</i>; <i>facility</i> <i>severity</i>; <i>match</i> "<i>regular-expression</i>"; <i>structured-data</i> { <i>brief</i>; } }</pre>
Hierarchy Level	[edit system syslog]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the logging of system messages to a file.
Options	<p><i>facility</i>—Class of messages to log. To specify multiple classes, include multiple <i>facility severity</i> statements.</p> <p><i>filename</i>—Filename that you specify with the show log command.</p> <p>Default: Filename messages</p> <p><i>severity</i>—Severity of the messages that belong to the facility specified by the paired <i>facility</i> name. Messages with severities at the specified level and higher are logged.</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"> • syslog on page 375

file (System Logging)


Syntax	<pre>file <i>filename</i> { <i>facility severity</i>; archive { <i>files number</i>; <i>size size</i>; (no-world-readable world-readable); } explicit-priority; match "<i>regular-expression</i>"; structured-data { brief; } }</pre>
Hierarchy Level	[edit system syslog]
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the logging of system messages to a file.
Options	<p>facility—Class of messages to log. To specify multiple classes, include multiple facility severity statements. For a list of the facilities, see Table 27 on page 159.</p> <p>file filename—File in the severity directory in which to log messages from the specified facility. To log messages to more than one file, include more than one file statement.</p> <p>severity—Severity of the messages that belong to the facility specified by the paired facility name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 28 on page 160.</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">• Directing System Log Messages to a Log File on page 146• Junos OS System Log Messages Reference

files

Syntax	<code>files <i>number</i>;</code>
Hierarchy Level	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for QFX Series switches.
Description	Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <i>logfile</i> , it closes the file, compresses it, and renames it to <i>logfile.0.gz</i> (for information about the maximum file size, see size). The utility then opens and writes to a new file called <i>logfile</i> . When the new file reaches the maximum size, the <i>logfile.0.gz</i> file is renamed to <i>logfile.1.gz</i> , and the new file is closed, compressed, and renamed <i>logfile.0.gz</i> . By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).
Options	<i>number</i> —Maximum number of archived files. Range: 1 through 1000 Default: 10 files
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying Log File Size, Number, and Archiving Properties on page 157 • Junos OS System Log Messages Reference • size on page 371

host (System)

Syntax	<pre>host (hostname other-routing-engine) { facility severity; exclude-hostname explicit-priority; facility-override facility; log-prefix string; match "regular-expression"; source-address source-address; structured-data { brief; } }</pre>
QFX Series and OCX Series	<pre>host (hostname { facility severity; explicit-priority; facility-override facility; log-prefix string; match "regular-expression"; port; source-address source-address; }</pre>
TX Matrix Router and EX Series Switches	<pre>host (hostname other-routing-engine scc-master) { facility severity; explicit-priority; facility-override facility; log-prefix string; match "regular-expression"; port; source-address source-address; }</pre>
TX Matrix Plus Router	<pre>host (hostname other-routing-engine sfc0-master) { facility severity; allow-duplicates; explicit-priority; facility-override facility; log-prefix string; match "regular-expression"; port; source-address source-address; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system syslog], [edit system syslog]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description	Configure the logging of system messages to a remote destination.
Options	<p>facility—Class of messages to log. To specify multiple classes, include multiple facility severity statements. For a list of the facilities, see Table 27 on page 159.</p> <p>hostname—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a host statement for each one.</p> <p>other-routing-engine—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.</p>
	<p> NOTE: The other-routing-engine option is not applicable to the QFX Series and OCX Series.</p>
	<p>port—Port number of the remote syslog server that can be modified.</p> <p>scc-master—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.</p> <p>severity—Severity of the messages that belong to the facility specified by the paired facility name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 28 on page 160.</p> <p>sfc0-master—(TX Matrix Plus routers only) On a T1600 or T4000 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.</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"> • <i>Directing System Log Messages to a Remote Machine or the Other Routing Engine</i> • <i>Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router</i> • <i>Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router</i> • <i>Junos OS System Log Messages Reference</i>

log-prefix (System)

Syntax	<code>log-prefix <i>string</i>;</code>
Hierarchy Level	[edit system syslog host]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Include a text string in each message directed to a remote destination.
Options	<i>string</i> —Text string to include in each message.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Adding a Text String to System Log Messages Directed to a Remote Destination on page 145• <i>Junos OS System Log Messages Reference</i>


match

Syntax	<code>match "regular-expression";</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i>], [edit logical-systems <i>logical-system-name</i> system syslog user (<i>username</i> *)], [edit system syslog file <i>filename</i>], [edit system syslog host <i>hostname</i> other-routing-engine scc-master)], [edit system syslog user (<i>username</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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.
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">• Using Regular Expressions to Refine the Set of Logged Messages on page 164

size (System)

Syntax	<code>size size;</code>
Hierarchy Level	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the maximum amount of data that the Junos OS logging utility writes to a log file <i>logfile</i> before archiving it (closing it, compressing it, and changing its name to <i>logfile.0.gz</i>). The utility then opens and writes to a new file called <i>logfile</i> . For information about the number of archive files that the utility creates in this way, see files .
Options	<p>size—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</p> <p>Syntax: <i>xk</i> to specify the number of kilobytes, <i>xm</i> for the number of megabytes, or <i>xg</i> for the number of gigabytes</p> <p>Range: 64 KB through 1 GB</p> <p>Default: 1 MB for MX Series routers the QFX Series, and the OCX Series</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"> • Specifying Log File Size, Number, and Archiving Properties on page 157 • Junos OS System Log Messages Reference • files on page 367

structured-data

Syntax	structured-data { brief; }
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i>], [edit system syslog file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, <i>The syslog Protocol</i> (http://tools.ietf.org/html/draft-ietf-syslog-protocol-23).
<div> NOTE: When this statement is included, other statements that specify the format for messages written to the file are ignored (the <code>explicit-priority</code> statement at the [edit system syslog file <i>filename</i>] hierarchy level and the <code>time-format</code> statement at the [edit system syslog] hierarchy level).</div>	
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">• <i>Logging Messages in Structured-Data Format</i>• <i>Junos OS System Log Messages Reference</i>• explicit-priority on page 363• time-format on page 376

syslog (System)

```

Syntax  syslog {
        allow-duplicates;
        archive {
            (binary-data | no-binary-data);
            files number;
            size maximum-file-size;
            start-time "YYYY-MM-DD.hh:mm";
            transfer-interval minutes;
            (world-readable | no-world-readable);
        }
        console {
            facility severity;
        }
        file filename {
            facility severity;
            explicit-priority;
            match "regular-expression";
            archive {
                (binary-data | no-binary-data);
                files number;
                size maximum-file-size;
                start-time "YYYY-MM-DD.hh:mm";
                transfer-interval minutes;
                (world-readable | no-world-readable);
            }
            structured-data {
                brief;
            }
        }
        host (hostname | other-routing-engine | scc-master) {
            facility severity;
            explicit-priority;
            facility-override facility;
            log-prefix string;
            match "regular-expression";
            source-address source-address;
            structured-data {
                brief;
            }
            port port number;
        }
        log-rotate-frequency frequency;
        server server name;
        source-address source-address;
        time-format (millisecond | year | year millisecond);
        user (username | *) {
            facility severity;
            match "regular-expression";
        }
    }

```


Hierarchy Level [edit system]

Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the types of system log messages to send to files, to a remote destination, to user terminals, or to the system console. The remaining statements are explained separately.
Options	archive —Define parameters for archiving log messages. console —Send log messages of a specified class and severity to the console. file —Send log messages to a named file. host —Remote location to be notified of specific log messages. log-rotate-frequency —Configure the interval for checking logfile size and archiving messages. server —Name of the system log server in the inet.0 routing instance. source-address —Include a specified address as the source address for log messages. time-format —Additional information to include in the system log time stamp. user —Notify a specific user of the log event.
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Junos OS System Log Overview</i>• <i>Junos OS System Log Messages Reference</i>• Overview of Single-Chassis System Logging Configuration on page 89

syslog (QFabric System)

Syntax	<pre> syslog { file <i>filename</i> { archive { size <i>maximum-file-size</i>; } explicit-priority; <i>facility severity</i>; match "<i>regular-expression</i>"; structured-data; } filter all { <i>facility severity</i>; match "<i>regular-expression</i>"; } host <i>hostname</i> { explicit-priority; <i>facility severity</i>; facility-override <i>facility</i>; log-prefix <i>string</i>; match "<i>regular-expression</i>"; structured-data; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	<p>Configure system log messages for the QFabric system.</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"> • Understanding the Implementation of System Log Messages on the QFabric System on page 91 • Directing System Log Messages to a Remote Machine on page 147

time-format

Syntax	<code>time-format (year millisecond year millisecond);</code>
Hierarchy Level	<code>[edit system syslog]</code>
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a file, console, or user statement at the <code>[edit system syslog]</code> hierarchy level. As of Junos OS Release 11.4, the additional time information is also sent to destinations configured by a host statement.</p> <p>By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, Aug 21 12:36:30. However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the <code>[edit system syslog time-format]</code> statement.</p>
<div> NOTE: When the <code>structured-data</code> statement is included at the <code>[edit system syslog file filename]</code> hierarchy level, this statement is ignored for the file.</div>	
Options	<p>millisecond—Include the millisecond in the timestamp.</p> <p>year—Include the year in the timestamp.</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">• <i>Including the Year or Millisecond in Timestamps</i>• <i>Junos OS System Log Messages Reference</i>• structured-data on page 372

user (System Logging)

Syntax	<pre> user (username *) { facility severity; match "regular-expression"; } </pre>
Hierarchy Level	[edit system syslog]
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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the logging of system messages to user terminals.
Options	<p>* (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.</p> <p>facility—Class of messages to log. To specify multiple classes, include multiple facility severity statements. For a list of the facilities, see Table 27 on page 159.</p> <p>severity—Severity of the messages that belong to the facility specified by the paired facility name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 28 on page 160.</p> <p>username—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one user statement.</p> <p>The remaining statement is 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"> • Directing System Log Messages to a User Terminal on page 147 • Junos OS System Logging Facilities and Message Severity Levels on page 159 • Junos OS System Log Messages Reference

CHAPTER 23

Monitoring Commands

- clear sflow collector statistics
- clear snmp history
- clear snmp statistics
- monitor traffic
- ping
- ping fabric multicast-flow
- ping fabric unicast-flow
- request snmp spoof-trap
- request snmp utility-mib clear instance
- request snmp utility-mib set instance
- show oam fabric flow-specification
- show oam fabric interfaces
- show log
- show sflow
- show sflow collector
- show sflow interface
- show snmp health-monitor
- show snmp inform-statistics
- show snmp mib
- show snmp rmon
- show snmp rmon history
- show snmp statistics
- show snmp v3
- traceroute fabric unicast-flow

clear sflow collector statistics

Syntax	clear sflow collector statistics
Release Information	Command introduced in Junos OS Release 11.3 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Clear the sample counters for all sFlow collectors.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Example: Monitoring Network Traffic Using sFlow Technology on page 116• Configuring sFlow Technology on page 115• show sflow collector on page 421
List of Sample Output	clear sflow collector statistics on page 380

Sample Output

clear sflow collector statistics

The following example shows two output examples for the **show sflow collector** command, one before and one after the **clear sflow collector statistics** command was issued.

```
user@host> show sflow collector
Collector      Udp-port      No. of samples
address
10.1.1.1       6343          3174
10.1.2.1       6343          3562
```

```
user@host> clear sflow collector statistics
```

```
user@host> show sflow collector
Collector      Udp-port      No. of samples
address
10.1.1.1       6343          0
10.1.2.1       6343          0
```


clear snmp history

Syntax	clear snmp history (<i>index</i> all)
Release Information	Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Delete the samples of Ethernet statistics collected for a history group.
Options	all —Clear all the entries in the history index. index —Clear the contents of the specified entry in the history index.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• clear snmp statistics on page 382

clear snmp statistics

Syntax	clear snmp statistics
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Clear Simple Network Management Protocol (SNMP) statistics.
Options	This command has no options.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show snmp statistics on page 439
List of Sample Output	clear snmp statistics on page 382
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
```


monitor traffic

Syntax monitor traffic
 <brief | detail | extensive>
 <absolute-sequence>
 <count *count*>
 <interface *interface-name*>
 <layer2-headers>
 <matching *matching*>
 <no-domain-names>
 <no-promiscuous>
 <no-resolve>
 <no-timestamp>
 <print-ascii>
 <print-hex>
 <resolve-timeout>
 <size *size*>

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display packet headers or packets received and sent from the Routing Engine.



NOTE:

- Using the **monitor-traffic** command can degrade router or switch performance.
 - Delays from DNS resolution can be eliminated by using the **no-resolve** option.
-
-



NOTE: This command is not supported on the QFabric system.

Options **none**—(Optional) Display packet headers transmitted through **fxp0**. On a TX Matrix Plus router, display packet headers transmitted through **em0**.

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

absolute-sequence—(Optional) Display absolute TCP sequence numbers.

count *count*—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The monitor traffic command quits automatically after displaying the number of packets specified.

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 37 on page 386](#).

Table 37: 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</i> mask <i>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 37: 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 38 on page 387](#).

Table 38: 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 38: 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 39 on page 389](#).



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 37 on page 386](#).
- 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 39: 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 390](#)
[monitor traffic detail count on page 390](#)
[monitor traffic extensive \(Absolute Sequence\) on page 390](#)
[monitor traffic extensive \(Relative Sequence\) on page 390](#)
[monitor traffic extensive count on page 390](#)
[monitor traffic interface on page 391](#)
[monitor traffic matching on page 391](#)
[monitor traffic \(TX Matrix Plus Router\) on page 391](#)
[monitor traffic \(QFX3500 Switch\) on page 392](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

monitor traffic count

```
user@host> monitor traffic count 2
listening on fxp0
04:35:49.814125 In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529478 win 16798 (DF)
04:35:49.814185
Out my-server.work.net.telnet > my-server.home.net.1295: P
1:38(37) ack 0 win 17680 (DF) [tos 0x10]
```

monitor traffic detail count

```
user@host> monitor traffic detail count 2
listening on fxp0
04:38:16.265864 In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529971 win 17678 (DF) (ttl 121, id 6812)
04:38:16.265926
Out my-server.work.net.telnet.telnet > my-server.home.net.1295: P 1:38(37) ack 0
win 17680 (DF) [tos 0x10] (ttl 6)
```

monitor traffic extensive (Absolute Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp" absolute-sequence
listening on fxp0
In 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 extensive (Relative Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp"
listening on fxp0
In 172.24.248.221.1680 > 192.168.4.210.23: . 396159737:396159737(0)
ack 1664980689 win 17574 (DF) (ttl 121, id 50003)
Out 192.168.4.210.23 > 172.24.248.221.1680: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10] (ttl 64, id 5394)
In 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 extensive count

```
user@host> monitor traffic extensive count 5 no-domain-names no-resolve
listening on fxp013:18:17.406933
In 192.168.4.206.2723610880 > 172.17.28.8.2049:
40 null (ttl 64, id 38367)13:18:17.407577
In 172.17.28.8.2049 > 192.168.4.206.2723610880:
```



```

reply ok 28 null (ttl 61, id 35495)13:18:17.541140
In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
0000 0100 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 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

List of Syntax [Syntax on page 394](#)
 [Syntax \(QFX Series\) on page 394](#)

Syntax `ping host`
 `<bypass-routing>`
 `<count requests>`
 `<detail>`
 `<do-not-fragment>`
 `<inet | inet6>`
 `<interface source-interface>`
 `<interval seconds>`
 `<logical-system logical-system-name>`
 `<loose-source value>`
 `<mac-address mac-address>`
 `<no-resolve>`
 `<pattern string>`
 `<rapid>`
 `<record-route>`
 `<routing-instance routing-instance-name>`
 `<size bytes>`
 `<source source-address>`
 `<strict >`
 `<strict-source value.>`
 `<tos type-of-service>`
 `<ttl value>`
 `<verbose>`
 `<vpls instance-name>`
 `<wait seconds>`

Syntax (QFX Series) `ping host`
 `<bypass-routing>`
 `<count requests>`
 `<detail>`
 `<do-not-fragment>`
 `<inet>`
 `<interface source-interface>`
 `<interval seconds>`
 `<logical-system logical-system-name>`
 `<loose-source value>`
 `<mac-address mac-address>`
 `<no-resolve>`
 `<pattern string>`
 `<rapid>`
 `<record-route>`
 `<routing-instance routing-instance-name>`
 `<size bytes>`
 `<source source-address>`
 `<strict>`
 `< strict-source value>`
 `<tos type-of-service>`
 `<ttl value>`
 `<verbose>`

<wait *seconds*>

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>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Check host reachability and network connectivity. The ping command sends Internet Control Message Protocol (ICMP) ECHO_REQUEST messages to elicit ICMP ECHO_RESPONSE messages from the specified host. Press Ctrl+c to interrupt a ping command.</p>
Options	<p>host—IP address or hostname of the remote system to ping.</p> <p>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.</p> <p>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.</p> <p>detail—(Optional) Include in the output the interface on which the ping reply was received.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> 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.</p> </div> <p>inet—(Optional) Ping Packet Forwarding Engine IPv4 routes.</p> <p>inet6—(Optional) Ping Packet Forwarding Engine IPv6 routes.</p> <p>interface source-interface—(Optional) Interface to use to send the ping requests.</p> <p>interval seconds—(Optional) How often to send ping requests. The range of values, in seconds, is 1 through infinity. The default value is 1.</p> <p>logical-system logical-system-name—(Optional) Name of logical system from which to send the ping requests.</p> <p>Alternatively, enter the set cli logical-system logical-system-name command and then run the ping command. To return to the main router or switch, enter the clear cli logical-system command.</p>

loose-source value—(Optional) Intermediate loose source route entry (IPv4). Open a set of values.

mac-address mac-address—(Optional) Ping the physical or hardware address of the remote system you are trying to reach.

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

pattern string—(Optional) Specify a hexadecimal fill pattern to include in the ping packet.

rapid—(Optional) Send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the **count** option.

record-route—(Optional) Record and report the packet's path (IPv4).

routing-instance routing-instance-name—(Optional) Name of the routing instance for the ping attempt.

size bytes—(Optional) Size of ping request packets. The range of values, in bytes, is 0 through 65,468. The default value is 56, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.

source source-address—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (lo.0).

strict—(Optional) Use the strict source route option (IPv4).

strict-source value—(Optional) Intermediate strict source route entry (IPv4). Open a set of values.

tos type-of-service—(Optional) Set the type-of-service (ToS) field in the IP header of the ping packets. The range of values is 0 through 255.

If the device configuration includes the **dscp-code-point value** statement at the **[edit class-of-service host-outbound-traffic]** hierarchy level, the configured DSCP value overrides the value specified in this command option. In this case, the ToS field of ICMP echo request packets sent on behalf of this command carries the DSCP value specified in the **dscp-code-point** configuration statement instead of the value you specify in this command option.

ttl value—(Optional) Time-to-live (TTL) value to include in the ping request (IPv6). The range of values is 0 through 255.

verbose—(Optional) Display detailed output.

vpls instance-name—(Optional) Ping the instance to which this VPLS belongs.

wait seconds—(Optional) Maximum wait time, in seconds, after the final packet is sent. If this option is not specified, the default delay is 10 seconds. If this option is used without the count option, a default count of 5 packets is used.

Required Privilege Level	network
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages</i>
List of Sample Output	ping hostname on page 397 ping hostname rapid on page 397 ping hostname size count on page 397
Output Fields	<p>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.</p>

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 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
```

ping hostname size count

```
user@host> ping skye size 200 count 5
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 fabric multicast-flow

Syntax	<code>ping fabric multicast-flow source-fmep-id <i>source-fmep-id</i> fma-name <i>fma-name</i> flow-spec-name <i>flow-specification-name</i> <verbose></code>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series.
Description	Send a fabric multicast ping command to the multicast group destination fabric maintenance endpoints (FMEPs) configured in the flow specification. Send a single PDU with a timeout after 1 second.
Options	<p>flow-spec-name <i>flow-specification-name</i>—Name of the flow specification that defines the protocol parameters (unicast or multicast) for the fabric ping operation.</p> <p>fma-name <i>fma-name</i>—Name of the FMA.</p> <p>source-fmep-id <i>source-fmep-id</i>—FMEP ID that is the source of the fabric ping operation.</p> <p>verbose—(Optional) Detailed version of the output display.</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"> • Overview of Internal Fabric Monitoring on page 29 • Configuring a Fabric Maintenance Association on page 103 • Configuring Flow Specifications on page 104 • fabric (OAM) on page 237 • ping fabric unicast-flow on page 400 • traceroute fabric unicast-flow on page 446
List of Sample Output	ping fabric multicast-flow on page 399
Output Fields	Table 40 on page 398 lists the output fields for the ping fabric-multicast-flow command. Output fields are listed in the approximate order in which they appear.

Table 40: ping fabric multicast-flow Output Fields

Field Name	Field Description
Using fabric flow-specification	Name of the flow specification.
Ethernet frame-size	Ethernet frame size in bytes.
Source-IP	MAC address of the source FMEP interface.
Destination-IP	MAC address of the destination FMEP interface.

Table 40: ping fabric multicast-flow Output Fields (*continued*)

Field Name	Field Description
Protocol	IP protocol.
received response from fmep-id	FMEP ID from which responses are received.

Sample Output

ping fabric multicast-flow

```
user@host> ping fabric multicast-flow source-fmep-id 3 fma-name fma1 flow-spec-name fspec2
verbose
```

```
Using fabric flow-specification: fspec2
```

```
Ethernet frame-size: 256
```

```
Source-IP: 87.238.205.21
```

```
Destination-IP: 225.0.0.1 IP
```

```
Protocol: 17
```

```
received response from fmep-id 32775...
```

```
received response from fmep-id 32794...
```

```
received response from fmep-id 32795...
```

```
sent 1 requests, received 3 responses
```


ping fabric unicast-flow

Syntax	<code>ping fabric unicast-flow fma-name <i>fma-name</i> source-fmep-id <i>source-fmep-id</i> dest-fmep-id <i>dest-fmep-id</i> flow-spec-name <i>flow-specification-name</i> <count <i>count</i>> <forced-fte-interface <i>fte-interface</i>> <verbose></code>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series.
Description	Send a unicast fabric ping command to the destination fabric maintenance endpoints (FMEPs) specified.
Options	<p>count <i>count</i>—(Optional) Number of fabric ping PDUs to send. The maximum PDU count is 5. The default PDU count is 1.</p> <p>dest-fmep-id <i>destination-fmep-id</i>—ID of the destination FMEP of the fabric ping operation.</p> <p>flow-spec-name <i>flow-specification-name</i>—Name of the flow specification that defines the protocol parameters (unicast or multicast) for the fabric ping operation.</p> <p>fma-name <i>fma-name</i>—Name of the FMA.</p> <p>forced-fte-interface <i>fte-interface</i>—(Optional) Forces the fabric ping operation to use the specified FTE interface to inject the PDU into the fabric instead of using the internal forwarding path lookup table to determine the FTE interface.</p> <p>source-fmep-id <i>source-fmep-id</i>—ID of the FMEP that is the source of the fabric ping operation.</p> <p>verbose—(Optional) Detailed version of the output display.</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">• Overview of Internal Fabric Monitoring on page 29• Configuring a Fabric Maintenance Association on page 103• Configuring Flow Specifications on page 104• fabric (OAM) on page 237• ping fabric multicast-flow on page 398• traceroute fabric unicast-flow on page 446
List of Sample Output	<p>ping fabric unicast-flow on page 401</p> <p>ping fabric unicast-flow (With Masking Enabled on the Flow Specification) on page 401</p>
Output Fields	<p>Table 41 on page 401 lists the output fields for the ping fabric-unicast-flow command. Output fields are listed in the approximate order in which they appear.</p>

Table 41: ping fabric unicast-flow Output Fields

Field Name	Field Description
Fabric flow ping between source <i>source-fmep-name</i> destination <i>destination-fmep-name</i>	Path of the unicast-flow ping between the source and detination FMEPs.
Using fabric flow-specification	Name of the flow specification.
Ethernet frame-size	Ethernet frame size in bytes.
Source-MAC	MAC address of the source FMEP interface.
Destination-MAC	MAC address of the destination FMEP interface.
Ethertype	EtherType protocol.
received response from fmep-id	ID of the FMEP sending the response.

Sample Output

ping fabric unicast-flow

```
user@host> ping fabric unicast-flow fma-name fma1 source-fmep-id 1 dest-fmep-id 2
flow-spec-name fspec1 verbose
```

```
Fabric flow ping between source ED1494 destination ED1497
Using fabric flow-specification: fspec1
Ethernet frame-size: 256
Source-MAC: 0:2:B1:61:3B:96
Destination-MAC: 0:26:78:90:70:21
EtherType: 8295
received response from fmep-id 2...
sent 1 requests, received 1 responses
```

ping fabric unicast-flow (With Masking Enabled on the Flow Specification)

```
user@host> ping fabric unicast-flow fma-name fma1 source-fmep-id 1 dest-fmep-id 2
flow-spec-name fspec1 verbose
```

```
Fabric flow ping between source ED1494 destination ED1497
Using fabric flow-specification: fspec1
Ethernet frame-size: 256
Source-MAC: 0:1:20:A0:0:1
Destination-MAC: 0:8A:3A:B3:7D:67
Source-MAC Mask: FF:F8:FF:FF:FF:FF
EtherType: 26785
Current Source-MAC value: 0:1:20:a0:0:1
received response from fmep-id 2...
Current Source-MAC value: 0:2:20:a0:0:1
received response from fmep-id 2...
Current Source-MAC value: 0:3:20:a0:0:1
received response from fmep-id 2...
Current Source-MAC value: 0:4:20:a0:0:1
received response from fmep-id 2...
Current Source-MAC value: 0:5:20:a0:0:1
received response from fmep-id 2...
```



```
Current Source-MAC value: 0:6:20:a0:0:1  
received response from fmep-id 2...  
Current Source-MAC value: 0:7:20:a0:0:1  
received response from fmep-id 2...  
sent 7 requests, received 7 responses
```


request snmp spoof-trap

Syntax	request snmp spoof-trap <trap> variable-bindings <object> <instance> <value>
Release Information	Command introduced in Junos OS Release 8.2. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.
Options	<p><trap>—Name of the trap to spoof.</p> <p>variable-bindings <object> <instance> <value>—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, ifIndex[14] = 14). Enclose the list of variable bindings in quotation marks (" ") and use a comma to separate each object name, instance, and value definition (for example, variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.</p> <p><dummy name>—A dummy trap name to display the list of available traps.</p> <p>Question mark (?)—Question mark? to display possible completions.</p>
Required Privilege Level	request
List of Sample Output	request snmp spoof-trap (with Variable Bindings) on page 403 request snmp spoof-trap (Illegal Trap Name) on page 403 request snmp spoof-trap (Question Mark ?) on page 407

Sample Output

request snmp spoof-trap (with Variable Bindings)

```
user@host> request snmp spoof-trap linkUp variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"
Spoof trap request result: trap sent successfully
```

request snmp spoof-trap (Illegal Trap Name)

```
user@host> request snmp spoof-trap xx
Spoof trap request result: trap not found
```

```
Allowed Traps:
ads1AtucInitFailureTrap
ads1AtucPerfESsThreshTrap
ads1AtucPerfLofsThreshTrap
ads1AtucPerfLolsThreshTrap
ads1AtucPerfLossThreshTrap
ads1AtucPerfLprsThreshTrap
ads1AtucRateChangeTrap
```


ads1AturPerfESsThreshTrap
ads1AturPerfLofsThreshTrap
ads1AturPerfLossThreshTrap
ads1AturPerfLprsThreshTrap
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
gmplsTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisIDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAccessAuthServerDisabled
jnxAccessAuthServerEnabled
jnxAccessAuthServiceDown
jnxAccessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared

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

jnxOspfV3IfStateChange
jnxOspfV3LsdbApproachingOverflow
jnxOspfV3LsdbOverflow
jnxOspfV3NbrRestartHelperStatusChange
jnxOspfV3NbrStateChange
jnxOspfV3NssaTranslatorStatusChange
jnxOspfV3RestartStatusChange
jnxOspfV3VirtIfConfigError
jnxOspfV3VirtIfRxBadPacket
jnxOspfV3VirtIfStateChange
jnxOspfV3VirtNbrRestartHelperStatusChange
jnxOspfV3VirtNbrStateChange
jnxOtnAlarmCleared
jnxOtnAlarmSet
jnxOverTemperature
jnxPmonOverloadCleared
jnxPmonOverloadSet
jnxPingEgressJitterThresholdExceeded
jnxPingEgressStdDevThresholdExceeded
jnxPingEgressThresholdExceeded
jnxPingIngressJitterThresholdExceeded
jnxPingIngressStdDevThresholdExceeded
jnxPingIngressThresholdExceeded
jnxPingRttJitterThresholdExceeded
jnxPingRttStdDevThresholdExceeded
jnxPingRttThresholdExceeded
jnxPortBpduErrorStatusChangeTrap
jnxPortLoopProtectStateChangeTrap
jnxPortRootProtectStateChangeTrap
jnxPowerSupplyFailure
jnxPowerSupplyOK
jnxRedundancySwitchover
jnxRmonAlarmGetFailure
jnxRmonGetOk
jnxSecAccessIfMacLimitExceeded
jnxSecAccessSdsRateLimitCrossed
jnxSonetAlarmCleared
jnxSonetAlarmSet
jnxSpSvcSetCpuExceeded
jnxSpSvcSetCpuOk
jnxSpSvcSetZoneEntered
jnxSpSvcSetZoneExited
jnxStormEventNotification
jnxSyslogTrap
jnxTemperatureOK
jnxVccpPortDown
jnxVccpPortUp
jnxVpnIfDown
jnxVpnIfUp
jnxVpnPwDown
jnxVpnPwUp
jnxl2aldGlobalMacLimit
jnxl2aldInterfaceMacLimit
jnxl2aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange


```

mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp
mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecI1lg1Lb1ThrshExcd
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

```


ads1AtucInitFailureTrap
ads1AtucPerfESsThreshTrap
ads1AtucPerfLofsThreshTrap
ads1AtucPerfLoIsThreshTrap
ads1AtucPerfLossThreshTrap
ads1AtucPerfLprsThreshTrap
ads1AtucRateChangeTrap
ads1AturPerfESsThreshTrap
ads1AturPerfLofsThreshTrap
ads1AturPerfLossThreshTrap
ads1AturPerfLprsThreshTrap
ads1AturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlsWTrapCircuitDown
dlsWTrapCircuitUp
---(more 10%)---

request snmp utility-mib clear instance

Syntax	request snmp utility-mib clear instance <i>name</i> object-type <i>type</i>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Clear the data stored in the specified container object in the SNMP Utility MIB.
Options	<p><i>name</i>—Name of the SNMP instance that is used to identify the data stored in the container object.</p> <p><i>object-type type</i>—Type of container object in which the data is stored. The following container object types are supported:</p> <ul style="list-style-type: none"> • counter—Stores a 32-bit counter value. • counter64—Stores a 64-bit counter value. • integer—Stores a 32-bit signed integer value. • unsigned-integer—Stores a 32-bit unsigned integer value.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Utility MIB on page 48 • Understanding the Implementation of SNMP on the QFabric System on page 42 • request snmp utility-mib set instance on page 410

request snmp utility-mib set instance

Syntax	<code>request snmp utility-mib set instance <i>name</i></code> <code>object-type <i>type</i></code> <code>object-value <i>value</i></code>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Store data in the specified container object in the SNMP Utility MIB. The data may be retrieved by SNMP operations.
Options	<p><i>name</i>—Name of the SNMP instance that is used to identify the data stored in the container object.</p> <p><i>object-type type</i>—Type of container object in which to store data. The following container object types are supported:</p> <ul style="list-style-type: none">• counter—Stores a 32-bit counter value.• counter64—Stores a 64-bit counter value.• integer—Stores a 32-bit signed integer value.• unsigned-integer—Stores a 32-bit unsigned integer value.• string—Stores an octet string value. <p><i>object-value value</i>—Data that is stored in the container object.</p>
Required Privilege Level	request
Related Documentation	<ul style="list-style-type: none">• Utility MIB on page 48• Understanding the Implementation of SNMP on the QFabric System on page 42• request snmp utility-mib clear instance on page 409

show oam fabric flow-specification

Syntax	show oam fabric flow-specification <flow-specification-name>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series.
Description	Display the fabric flow specifications that are configured in a QFabric system Node group.
Options	<i>flow-specification-name</i> —(Optional) Name of a flow specification.
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"> • Overview of Internal Fabric Monitoring on page 29 • Configuring a Fabric Maintenance Association on page 103 • Configuring Flow Specifications on page 104 • fabric (OAM) on page 237 • ping fabric multicast-flow on page 398 • ping fabric unicast-flow on page 400 • traceroute fabric unicast-flow on page 446
List of Sample Output	show oam fabric flow-specification (All) on page 412 show oam fabric flow-specification (Flow Specification Specified) on page 413
Output Fields	Table 42 on page 411 lists the output fields for the show oam fabric flow-specification command. Output fields are listed in the approximate order in which they appear.

Table 42: show oam fabric flow-specification Output Fields

Field Name	Field Description
Flow specification name	Name of the flow specification.
Type	Flow specification type: <ul style="list-style-type: none"> • Ethernet • Ethernet Unicast IPV4 • Multicast IPV4 • Multicast VLAN flood
Ethernet frame size	Ethernet frame size in bytes.
Ether type	EtherType protocol.
Source-MAC	MAC address of the source FMEP interface.

Table 42: show oam fabric flow-specification Output Fields (*continued*)

Field Name	Field Description
Source-MAC Mask	MAC address mask of the source FMEP interface.
Destination-MAC	MAC address of the destination FMEP interface.
Destination-MAC Mask	MAC address mask of the destination FMEP interface.
Source-IP	IP address of the source FMEP interface.
Source-IP Mask	IP address mask of the source FMEP interface.
Destination-IP	IP address of the destination FMEP interface.
Destination-IP mask	IP address mask of the destination FMEP interface.
IP-Protocol	IPv4 protocol configured.
Source-L4-Port	Source TCP or UDP port.
Destination-L4-Port	Destination TCP or UDP port.
Destination multicast group IP	IP address of the destination multicast group.

Sample Output

show oam fabric flow-specification (All)

```

user@host> show oam fabric flow-specification

Flow specification name : fspec1 Type : Ethernet
  Ethernet frame size : Unspecified
  Ether type : Unspecified
  Source-MAC : Unspecified
  Source-MAC Mask : Unspecified
  Destination-MAC : Unspecified
  Destination-MAC Mask : Unspecified
Flow specification name : fspec2 Type : Ethernet
  Ethernet frame size : Unspecified
  Ether type : 1792
  Source-MAC : 0:0:a0:f0:cc:22
  Source-MAC Mask : Unspecified
  Destination-MAC : 0:11:22:33:a0:e2
  Destination-MAC Mask : Unspecified
Flow specification name : fspec3 Type : Ethernet Unicast IPV4
  Ethernet frame size : Unspecified
  Source-IP : 121.0.0.1
  Source-IP Mask : Unspecified
  Destination-IP : 132.1.0.1
  Destination-IP Mask : Unspecified
  Destination-mac : Unspecified
  IP-protocol : TCP
  Source-L4-port : 270

```



```
Destination-L4-port : Unspecified
Flow specification name : fspec4 Type : Multicast IPv4
Ethernet frame size : Unspecified
Source IP : 100.0.0.23
Destination multicast group IP: 225.0.0.1
Flow specification name : fspec5 Type : Multicast VLAN flood
Ethernet frame size : Unspecified
```

show oam fabric flow-specification (Flow Specification Specified)

```
user@host> show oam fabric flow-specification fspec3
```

```
Flow specification name : fspec3 Type : Ethernet Unicast IPv4
Ethernet frame size : Unspecified
Source-IP : 121.0.0.1
Source-IP Mask : Unspecified
Destination-IP : 132.1.0.1
Destination-IP Mask : Unspecified
Destination-mac : Unspecified
IP-protocol : TCP
Source-L4-port : 270
Destination-L4-port : Unspecified
```


show oam fabric interfaces

Syntax	<pre>show oam fabric interfaces <interface-name> <fabric-maintenance-association fma-name> <brief></pre>
Release Information	Command introduced in Junos OS Release 12.2 for the QFX Series.
Description	<p>Display the fabric maintenance associations (FMAs) and fabric maintenance endpoints (FMEPs) that are configured in a QFabric system Node group.</p> <p>If you do not specify an interface, display information for an FMA (if one is specified) or all FMAs configured in the Node group.</p>
Options	<p>brief—(Optional) Summarized version of the output.</p> <p>fabric-maintenance-association <i>fma-name</i>—(Optional) Name of a specific FMA.</p> <p>interface-name—(Optional) Name of a specific interface.</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"> • Overview of Internal Fabric Monitoring on page 29 • Configuring a Fabric Maintenance Association on page 103 • Configuring Flow Specifications on page 104 • fabric (OAM) on page 237 • ping fabric multicast-flow on page 398 • ping fabric unicast-flow on page 400 • traceroute fabric unicast-flow on page 446
List of Sample Output	show oam fabric interfaces on page 415
Output Fields	<p>Table 43 on page 414 lists the output fields for the show oam fabric interfaces command. Output fields are listed in the approximate order in which they appear.</p>

Table 43: show oam fabric interfaces Output Fields

Field Name	Field Description
Interface-name	Name of the interface.
Fabric-Maintenance Association	FMA name.
VLAN	VLAN name.
Interface state	State of the interface: Up or down.

Table 43: show oam fabric interfaces Output Fields (*continued*)

Field Name	Field Description
MEP Identifier	FMEP identifier.
MEP Name	FMEP name.

Sample Output

show oam fabric interfaces

```
user@host> show oam fabric interfaces
```

Interface-name	Fabric-Maintenance Association	VLAN	Interface state	MEP Identifier	MEP Name
ED1479:NULL	fma-default	*	up	32774	
fmeop-default-ED1479					
ED1494:NULL	fma-default	*	up	32773	
fmeop-default-ED1494					
ED1494:xe-0/0/7.0	fma1	v100	up	1	
ED1497:NULL	fma-default	*	up	32775	
fmeop-default-ED1497					
ED1497:xe-0/0/8.0	fma1	v100	up	2	
P3613-C:NULL	fma-default	*	up	32777	
fmeop-default-P3613-C					

show log

List of Syntax	Syntax on page 416 Syntax (QFX Series and OCX Series) on page 416 Syntax (TX Matrix Routers) on page 416
Syntax	<code>show log</code> <code><filename user <username>></code>
Syntax (QFX Series and OCX Series)	<code>show log filename</code> <code><device-type (device-id device-alias)></code>
Syntax (TX Matrix Routers)	<code>show log</code> <code><all-lcc lcc number scc></code> <code><filename user <username>></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Option <i>device-type (device-id device-alias)</i> is introduced in Junos OS Release 13.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	List log files, display log file contents, or display information about users who have logged in to the router or switch.
Options	none —List all log files. <all-lcc lcc number scc> —(TX Matrix routers only) (Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace <i>number</i> with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis). device-type —(QFabric system only) (Optional) Display log messages for only one of the following device types: <ul style="list-style-type: none">• director-device—Display logs for Director devices.• infrastructure-device—Display logs for the logical components of the QFabric system infrastructure, including the diagnostic Routing Engine, fabric control Routing Engine, fabric manager Routing Engine, and the default network Node group and its backup (NW-NG-0 and NW-NG-0-backup).• interconnect-device—Display logs for Interconnect devices.• node-device—Display logs for Node devices.



NOTE: If you specify the **device-type** optional parameter, you must also specify either the **device-id** or **device-alias** optional parameter.

(device-id | device-alias)—If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).

filename—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.



NOTE: The *filename* parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of messages.

user <username>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include *username*, display logging information about the specified user.

Required Privilege Level trace

List of Sample Output [show log on page 417](#)
[show log filename on page 417](#)
[show log filename \(QFabric System\) on page 418](#)
[show log user on page 418](#)

Sample Output

show log

```
user@host> show log
total 57518
-rw-r--r-- 1 root bin      211663 Oct  1 19:44 dcd
-rw-r--r-- 1 root bin      999947 Oct  1 19:41 dcd.0
-rw-r--r-- 1 root bin      999994 Oct  1 17:48 dcd.1
-rw-r--r-- 1 root bin      238815 Oct  1 19:44 rpd
-rw-r--r-- 1 root bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r-- 1 root bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r-- 1 root bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r-- 1 root bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r-- 1 root bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r-- 1 root bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r-- 1 root bin     1056350 Sep 30 07:04 rpd.6
-rw-r--r-- 1 root bin     1048876 Sep 30 03:21 rpd.7
-rw-rw-r-- 1 root bin       19656 Oct  1 19:37 wtmp
```

show log filename

```
user@host> show log rpd
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct  1 18:00:18
Oct  1 18:00:19 KRT rcv len 56 V9 seq 148 op add Type route/if af 2 addr
13.13.13.21 nhop type local nhop 13.13.13.21
Oct  1 18:00:19 KRT rcv len 56 V9 seq 149 op add Type route/if af 2 addr
13.13.13.22 nhop type unicast nhop 13.13.13.22
Oct  1 18:00:19 KRT rcv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct  1 18:00:19 KRT rcv len 144 V9 seq 151 op chnge Type ifdev devindex 44
```



```

Oct  1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...

```

show log filename (QFabric System)

```

user@qfabric> show log messages
Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486
  chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486
  chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
  chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242726)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
  chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 242757)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default__NW-INE-0_REO_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default__NW-INE-0_REO_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491
  chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)

```

show log user

```

user@host> show log user
darius  mg2546                Thu Oct  1 19:37   still logged in
darius  mg2529                Thu Oct  1 19:08 - 19:36 (00:28)
darius  mg2518                Thu Oct  1 18:53 - 18:58 (00:04)
root    mg1575                Wed Sep 30 18:39 - 18:41 (00:02)
root    ttyp2      jun.site.per Wed Sep 30 18:39 - 18:41 (00:02)
alex    ttyp1      192.168.1.2   Wed Sep 30 01:03 - 01:22 (00:19)

```


show sflow

Syntax	show sflow <collector> <interface>
Release Information	Command introduced in Junos OS Release 11.3 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display sFlow configuration information.
Options	<p>none—Display all sFlow configuration information.</p> <p>collector—(Optional) Display a list of configured sFlow collectors and their properties.</p> <p>interface—(Optional) Display the interfaces on which sFlow technology is enabled and the sampling parameters.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show sflow interface on page 422 • show sflow collector on page 421 • clear sflow collector statistics on page 380 • Example: Monitoring Network Traffic Using sFlow Technology on page 116 • Configuring sFlow Technology on page 115
List of Sample Output	show sflow on page 420
Output Fields	Table 44 on page 419 lists the output fields for the show sflow command. Output fields are listed in the approximate order in which they appear.

Table 44: show sflow Output Fields

Field Name	Field Description	Level of Output
sFlow	Status of the feature: Enabled or Disabled .	All levels
Sample limit	Number of packets sampled per second. This sample limit cannot be configured and is set to 300 packets per second.	All levels
Polling interval	Interval at which the sFlow agent polls the interface.	All levels
Sample rate egress	Rate at which egress packets are sampled.	All levels
Sample rate ingress	Rate at which ingress packets are sampled.	All levels
Agent ID	IP address assigned to the sFlow agent.	All levels

Table 44: show sflow Output Fields (*continued*)

Field Name	Field Description	Level of Output
Source IP address	Source IP address for the sFlow packets.	All levels

Sample Output

show sflow

```
user@host> show sflow
```

```
sFlow           : Enabled
Sample limit    : 300 packets/second
Polling interval : 20 second
Sample rate egress : 1:2048: Disabled
Sample rate ingress : 1:1000: Enabled
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 11.3 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display a list of configured sFlow collectors and their properties.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear sflow collector statistics on page 380 • show sflow on page 419 • show sflow interface on page 422 • Example: Monitoring Network Traffic Using sFlow Technology on page 116 • Configuring sFlow Technology on page 115
List of Sample Output	show sflow collector on page 421
Output Fields	Table 45 on page 421 lists the output fields for the show sflow collector command. Output fields are listed in the approximate order in which they appear.

Table 45: show sflow collector Output Fields

Field Name	Field Description	Level of Output
Collector address	IP address of the collector.	All levels
UDP-Port	UDP port number of the collector.	All levels
No. of samples	Number of samples collected.	All levels

Sample Output

show sflow collector

```
user@host> show sflow collector
```

```

Collector      Udp-port      No. of samples
address
10.204.32.46   6343          1000
100.204.32.76  3400          1000
```


show sflow interface

Syntax	show sflow interface
Release Information	Command introduced in Junos OS Release 11.3 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display the interfaces on which sFlow is enabled and the sampling parameters for the interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show sflow on page 419 • show sflow collector on page 421 • Example: Monitoring Network Traffic Using sFlow Technology on page 116 • Configuring sFlow Technology on page 115
List of Sample Output	show sflow interface (QFX3500 Switch in Standalone Mode) on page 422 show sflow interface (QFabric System) on page 423
Output Fields	Table 46 on page 422 lists the output fields for the show sflow interface command. Output fields are listed in the approximate order in which they appear.

Table 46: show sflow interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which sFlow technology is enabled.	All levels
Status Egress	Indicates whether an egress sample rate is enabled.	All levels
Status Ingress	Indicates whether an ingress sample rate is enabled.	All levels
Sample rate Egress	Rate at which egress packets are sampled.	All levels
Sample rate Ingress	Rate at which ingress packets are sampled.	All levels
Adapted sample rate Egress	Adapted rate at which egress packets are sampled.	All levels
Adapted sample rate Ingress	Adapted rate at which ingress packets are sampled.	All levels
Polling-interval	Interval at which the sFlow agent polls the interface.	All levels

Sample Output

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
```


Interface	Status	Sample rate		Adapted sample rate		Polling-interval	
		Egress	Ingress	Egress	Ingress		
xe-0/0/0.0	Enabled	Disabled	1000	2048	1000	2048	20
xe-1/0/1.0	Enabled	Disabled	1000	2048	1000	2048	20

Sample Output

show sflow interface (QFabric System)

```
user@host> show sflow interface
```

Interface	Status	Sample rate		Adapted sample rate		Polling-interval
		Egress	Ingress	Egress	Ingress	
node1:xe-0/0/0.0	Enabled	Disabled	1000	2048	1000	2048
node2:xe-1/0/1.0	Enabled	Disabled	1000	2048	1000	2048
node4:xe-1/0/0.0	Enabled	Disabled	1000	2048	1000	2048

show snmp health-monitor

Syntax	show snmp health-monitor <alarms (brief detail) logs>
Release Information	Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.
Options	<p>none—Display information about all health monitor alarms and logs.</p> <p>alarms (brief detail)—(Optional) Display information about health monitor alarms. Optionally, specify brief or detailed information about the alarms.</p> <p>logs—(Optional) Display information about health monitor logs.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Understanding Health Monitoring on page 55 • Configuring Health Monitoring on page 132
List of Sample Output	show snmp health-monitor on page 426 show snmp health-monitor alarms detail on page 426
Output Fields	Table 47 on page 424 describes the output fields for the show snmp health-monitor command. Output fields are listed in the approximate order in which they appear.

Table 47: 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 47: 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 <i>absolute value</i> or <i>delta value</i> .	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. <i>falling alarm</i> Value of the alarm is below or equal to the falling threshold and the startup type is either <i>falling alarm</i> or <i>rising or falling alarm</i>. 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 <i>falling alarm</i>. Value of the alarm is below or equal to the falling threshold and the startup type is <i>rising alarm</i>. 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 47: 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	Index number of the event triggered when the rising threshold is crossed.	detail
Falling event index	Index number of the event triggered when the falling threshold is crossed. Details include the value of the falling event instance and the state of the falling event instance.	detail

Sample Output

show snmp health-monitor

```

user@switch> show snmp health-monitor

Alarm
Index  Variable description                                Value State
-----
32768  Health Monitor: root file system utilization
      jnxHrStoragePercentUsed.1                        59 active

32769  Health Monitor: /config file system utilization
      jnxHrStoragePercentUsed.2                        0 active

32770  Health Monitor: RE 0 CPU utilization
      jnxOperatingCPU.9.1.0.0                          9 falling threshold

32772  Health Monitor: RE 0 memory utilization
      jnxOperatingBuffer.9.1.0.0                       23 active

32774  Health Monitor: Max Kernel Memory Used (%)
      jnxBoxKernelMemoryUsedPercent.0                  3 active
Event Index: 32768
Description: Health Monitor: RE 0 CPU utilization crossed falling threshold
70 (value: 5), (variable: jnxOperatingCPU.9.1.0.0)
Time: 2011-01-09 19:18:35 PST

```

show snmp health-monitor alarms detail

```

user@switch> 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: 59
  Instance State: active

```

Alarm Index 32769:

```

Variable name              jnxHrStoragePercentUsed.2
Variable OID              1.3.6.1.4.1.2636.3.31.1.1.1.2
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: 9
  Instance State: falling threshold

```

Alarm Index 32772:

```

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: 23
  Instance State: active

```

Alarm Index 32774:

```

Variable name              jnxBoxKernelMemoryUsedPercent.0
Variable OID              1.3.6.1.4.1.2636.3.1.16.0
Sample type               absolute value

```


Startup alarm	rising alarm
Owner	Health Monitor: Max Kernel Memory Used (%)
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: 3	
Instance State: active	

show snmp inform-statistics

Syntax	show snmp inform-statistics
Release Information	<p>Command introduced in Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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 429
Output Fields	Table 48 on page 429 describes the output fields for the show snmp inform-statistics command. Output fields are listed in the approximate order in which they appear.

Table 48: 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 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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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 432</p> <p>show snmp mib get (Multiple Objects) on page 432</p> <p>show snmp mib get (Layer 2 Policer) on page 432</p> <p>show snmp mib get-next on page 432</p> <p>show snmp mib get-next (Specify an OID) on page 432</p> <p>show snmp mib walk on page 432</p> <p>show snmp mib walk (QFX Series) on page 432</p> <p>show snmp mib walk decimal on page 433</p> <p>show snmp mib walk (ASCII) on page 433</p> <p>show snmp mib walk (Multiple Indices) on page 433</p> <p>show snmp mib walk decimal (Multiple Indices) on page 433</p>
Output Fields	Table 49 on page 432 describes the output fields for the show snmp mib command. Output fields are listed in the approximate order in which they appear.

Table 49: 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 (Multiple Objects)

```
user@host> show snmp mib get ?sysObjectID.0 sysUpTime.0?
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

show snmp mib get (Layer 2 Policer)

```
user@host> show snmp mib get ifInOctets.25970
ifInOctets.25970 = 7545720
```

show snmp mib get-next

```
user@host> show snmp mib get-next jnxMibs
jnxBoxClass.0 = jnxProductLineM20.0
```

show snmp mib get-next (Specify an OID)

```
user@host> show snmp mib get-next 1.3.6.1
sysDescr.0 = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper
Networks, Inc.
```

show snmp mib walk

```
user@host> show snmp mib walk system
sysDescr.0 = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004
Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
sysContact.0 = Your contact
sysName.0 = my router
sysLocation.0 = building 1
sysServices.0 = 4
```

show snmp mib walk (QFX Series)

```
user@switch> show snmp mib walk system
sysDescr.0 = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0 = 138980301
sysContact.0 = System Contact
```



```

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

```

show snmp mib walk decimal

```

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

```

show snmp mib walk (ASCII)

```

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

```

show snmp mib walk (Multiple Indices)

```

show snmp mib walk ascii jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.....

```

show snmp mib walk decimal (Multiple Indices)

```

show snmp mib walk ascii jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.....

```


show snmp rmon

Syntax	<pre>show snmp rmon <alarms (brief detail)> <events (brief detail)> <logs></pre>
Release Information	<p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms, events, and logs.
Options	<p>none—Display information about all RMON alarms and events.</p> <p>brief detail—(Optional) Display brief or detailed information about RMON alarms or events.</p> <p>alarms—(Optional) Display information about RMON alarms.</p> <p>events—(Optional) Display information about RMON events.</p> <p>logs—(Optional) Display information about RMON monitoring logs.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • RMON MIB Event, Alarm, Log, and History Control Tables on page 53 • Monitoring RMON MIB Tables on page 179 • Configuring RMON Alarms and Events on page 130 • Understanding RMON on page 51 • clear snmp statistics on page 382 • clear snmp history on page 381 • show snmp rmon history on page 438
List of Sample Output	<p>show snmp rmon on page 436</p> <p>show snmp rmon alarms detail on page 437</p> <p>show snmp rmon events detail on page 437</p> <p>show snmp rmon logs on page 437</p>
Output Fields	<p>Table 50 on page 434 describes the output fields for the show snmp rmon command. Output fields are listed in the approximate order in which they appear.</p>

Table 50: show snmp rmon Output Fields

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

Table 50: 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	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 50: 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  Variable description                               Value State

      5  monitor
         jnxOperatingCPU.9.1.0.0                       5 falling threshold

Event
Index  Type                               Last Event
      1  log and trap                     2009-07-10 11:34:17 PDT
Event Index: 1
Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
Time: 2009-07-10 11:34:07 PDT

```


Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
 (variable: jnxOperatingCPU.9.1.0.0, value: 5)
 Time: 2009-07-10 11:34:17 PDT

show snmp rmon alarms detail

```
user@host> show snmp rmon alarms detail
Alarm Index 5:
  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 or falling alarm
  Owner                   monitor

  Creator                 CLI
  State                   active
  Sample interval         5 seconds
  Rising threshold        90
  Falling threshold       75
  Rising event index      1
  Falling event index     1
  Instance Value: 4
  Instance State: falling threshold
```

show snmp rmon events detail

```
user@host> show snmp rmon events detail
Event Index 1:
  Description             rmon event
  Type                    log and trap
  Community               rmon-trap-group
  Last event              2009-07-10 11:34:17 PDT
  Creator                 CLI
  State                   active
```

show snmp rmon logs

```
user@host> show snmp rmon logs
Event Index: 1
  Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
  (variable: jnxOperatingCPU.9.1.0.0, value: 100)
  Time: 2009-07-10 11:34:07 PDT
  Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
  (variable: jnxOperatingCPU.9.1.0.0, value: 5)
  Time: 2009-07-10 11:34:17 PDT
```


show snmp rmon history

Syntax	<code>show snmp rmon history</code> <code><history-index></code> <code>sample-index <sample-index></code>
Release Information	Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display the contents of the RMON history group.
Options	none —Display all the entries in the RMON history group. history-index —(Optional) Display the contents of the specified entry in the RMON history group. sample-index sample-index —(Optional) Display the statistics collected for the specified sample within the specified entry in the RMON history group.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• RMON MIB Event, Alarm, Log, and History Control Tables on page 53• Monitoring RMON MIB Tables on page 179• Configuring RMON Alarms and Events on page 130• Understanding RMON on page 51• clear snmp statistics on page 382• clear snmp history on page 381• show snmp rmon on page 434

show snmp statistics

Syntax	show snmp statistics
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>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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 382
List of Sample Output	show snmp statistics on page 442
Output Fields	<p>Table 51 on page 439 describes the output fields for the show snmp statistics command.</p> <p>Output fields are listed in the approximate order in which they appear.</p>

Table 51: 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 51: 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 51: 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 51: 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 in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display the Simple Network Management Protocol version 3 (SNMPv3) operating configuration.
Options	<p>none—Display all of the SNMPv3 operating configuration.</p> <p>access—(Optional) Display SNMPv3 access information.</p> <p>brief detail—(Optional) Display brief or detailed information about SNMPv3 access information.</p> <p>community—(Optional) Display SNMPv3 community information.</p> <p>general—(Optional) Display SNMPv3 general information.</p> <p>groups—(Optional) Display SNMPv3 security-to-group information.</p> <p>notify <filter>—(Optional) Display SNMPv3 notify information and, optionally, notify filter information.</p> <p>target <address parameters>—(Optional) Display SNMPv3 target information and, optionally, either target address or target parameter information.</p> <p>users—(Optional) Display SNMPv3 user information.</p>
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
Related Documentation	<ul style="list-style-type: none"> • SNMPv3 Overview on page 49 • Minimum SNMPv3 Configuration on a Device Running Junos OS on page 50 • Configuring Access Privileges for a Group on page 134
List of Sample Output	show snmp v3 on page 444
Output Fields	Table 52 on page 444 describes the output fields for the show snmp v3 command. Output fields are listed in the approximate order in which they appear.

Table 52: show snmp v3 Output Fields

Field Name	Field Description
Local engine	<p>Information about the local SNMP engine configuration:</p> <ul style="list-style-type: none"> • Local engine ID—Unique Identifier of the local SNMPv3 engine. • Engine boots—Number of times the local SNMPv3 engine has rebooted or reinitialized since this engine ID was configured. • 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 (local engine)	<p>Information about the local SNMP engine ID and the associated users:</p> <ul style="list-style-type: none"> • User—SNMPv3 username. • Auth/Priv—Authentication and encryption algorithm that is configured for the user. • Storage—Indicates whether a username is saved to the configuration file (nonvolatile) or not saved (volatile). Applies only to users with active status. • Status—Status of the user as listed in the SNMPv3 user table. Only rows with an active status in the table are used by the SNMPv3 engine.
Engine ID (remote engine)	<p>Information about a remote SNMP engine, associated users, user groups, and user access policies:</p> <ul style="list-style-type: none"> • User—SNMPv3 username. • Auth/Priv—Authentication and encryption algorithm that is configured for the user. • Storage—Indicates whether a username is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status. • Status—Status of a new user that has been activated. Only users with an active status can use SNMPv3. • Group name—Name of a group of users for which the configured access privileges apply. • Security model—Security model (such as usm, v1, v2c, or any) that is configured for the group. The security model is used with the security name to ensure messaging security. • Security name—Security name that is associated with a user, and which is used with the security model to ensure messaging security. • Storage type—Indicates whether a username is saved to the configuration file (nonvolatile) or not saved (volatile). Applies only to users with active status. • Status—Status of a user in a group. Only users with an active status can use SNMPv3.
Access control	<p>Information about access control:</p> <ul style="list-style-type: none"> • Group name—Name of a group of users for which the configured access privileges apply. • Context prefix—SNMPv3 context for which the configured access privileges apply. • Security model/level—Security model and security level combination that is configured for user access privileges. • Read view—Identifies the MIB view used for SNMPv3 read operations. • Write view—Identifies the MIB view used for SNMPv3 write operations. • Notify view—Identifies the MIB view used for outbound SNMP notifications.

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 model	Security name	Storage type	Status
g1	usm	user1	nonvolatile	active
g2	usm	user2	nonvolatile	active
g3	usm	user3	nonvolatile	active

Access control:

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

traceroute fabric unicast-flow

Syntax `traceroute fabric unicast-flow flow-spec-name flow-specification-name fma fma-name
 <source-fmep fmep-name>
 <dest-fmep fmep-name>
 <forced-fte-interface fte-interface>
 <count count>
 <verbose>`

Release Information Command introduced in Junos OS Release 12.2 for the QFX Series.

Description Trace the path taken by a specific unicast flow (ping) operation across a VLAN on the QFabric system from a source maintenance endpoint (FMEP) to a destination FMEP. The source and destination FMEPs may be on the same Node device, different Node devices connected to the same Interconnect device, or different Node devices connected to different Interconnect devices.

The flow path is the sequence of Packet Forwarding Engine forwarding hops along which the protocol data unit (PDU) travels. The hop-by-hop sequence and number of hops are reported in terms of fabric maintenance intermediate points (FMIPs), which are interfaces on the Packet Forwarding Engine of the Interconnect device. An FMIP sends a response to the source FMEP when the traceroute PDU is received.



NOTE: This command is not supported on the QFX3000-M QFabric system.

Options `dest-fmep-id source-fmep-id`—(Optional) ID of the destination FMEP of the traceroute operation.

`flow-spec-name flow-specification-name`—Name of the flow specification that defines the parameters of the traceroute operation.

`fma-name fma-name`—Name of the FMA that associates a VLAN with the FMEPs.

`forced-fte-interface fte-interface`—(Optional) Option to force the fabric ping operation to use the specified FTE interface to inject the PDU into the fabric instead of using the internal forwarding path lookup table to determine the FTE interface.

`source-fmep-id source-fmep-id`—(Optional) ID of the FMEP that is the source of the traceroute operation.

`verbose`—(Optional) Detailed version of the output display.

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

Related Documentation

- [Overview of Internal Fabric Monitoring on page 29](#)
- [Configuring a Fabric Maintenance Association on page 103](#)

- [Configuring Flow Specifications on page 104](#)
- [fabric \(OAM\) on page 237](#)
- [ping fabric multicast-flow on page 398](#)
- [ping fabric unicast-flow on page 400](#)

List of Sample Output [traceroute fabric unicast-flow on page 447](#)
[traceroute fabric unicast-flow \(Verbose\) on page 447](#)

Output Fields [Table 53 on page 447](#) lists the output fields for the **traceroute fabric-unicast-flow** command. Output fields are listed in the approximate order in which they appear.

Table 53: traceroute fabric unicast-flow Output Fields

Field Name	Field Description
Fabric flow traceroute between source <i>source-fmep-name</i> destination <i>destination-fmep-name</i>	Source and destination FMEP names.
Using fabric flow-specification	Name of the flow specification.
Ethernet frame-size	Ethernet frame size.
Source-MAC	MAC address of the source FMEP interface.
Destination-MAC	MAC address of the destination FMEP interface.
Ethertype	EtherType protocol.
Received response from fmip-id, interface	FMIP identifier and interface name of the FMIP that received the PDU and responded to the source FMEP.
Received total <i>number</i> responses	Number of responses that are received after the traceroute operation has finished.

Sample Output

traceroute fabric unicast-flow

```
user@host> traceroute fabric unicast-flow fma-name fma1 source-fmep-id 1 dest-fmep-id 2
flow-spec-name fspec1
Received response from fmip-id 128.40.0.8, interface A0003:0/1/2
Received response from fmip-id 128.128.0.8, interface A0003:0/0/8
Received response from fmep-id 2
Received total 3 responses
```

Sample Output

traceroute fabric unicast-flow (Verbose)

```
user@host> traceroute fabric unicast-flow fma-name fma1 source-fmep-id 1 dest-fmep-id 2
flow-spec-name fspec1 verbose
```



```
Fabric flow traceroute between source ED1494 destination ED1497
Using fabric flow-specification: fspec1
Ethernet frame-size: 256
Source-MAC: 0:EF:7:99:85:10
Destination-MAC: 0:D3:A6:11:39:21
Ethertype: 11564
Received response from fmip-id 128.40.0.8, interface A0003:0/1/2
Received response from fmip-id 128.128.0.8, interface A0003:0/0/8
Received response from fmep-id 2
Received total 3 responses
```